A Survey of Trust in Social Networks

WANITA SHERCHAN, IBM Research- Australia
SURYA NEPAL and CECILE PARIS, CSIRO ICT Centre

Web-based social networks have become popular as a medium for disseminating information and connecting like-minded people. The public accessibility of such networks with the ability to share opinions, thoughts, information, and experience offers great promise to enterprises and governments. In addition to individuals using such networks to connect to their friends and families, governments and enterprises have started exploiting these platforms for delivering their services to citizens and customers. However, the success of such attempts relies on the level of trust that members have with each other as well as with the service provider. Therefore, trust becomes an essential and important element of a successful social network. In this article, we present the first comprehensive review of social and computer science literature on trust in social networks. We first review the existing definitions of trust and define *social trust* in the context of social networks. We then discuss recent works addressing three aspects of social trust: *trust information collection*, *trust evaluation*, and *trust dissemination*. Finally, we compare and contrast the literature and identify areas for further research in social trust.

Categories and Subject Descriptors: A.1 [**Introductory and Survey**]; C.2.4 [**Computer-Communication Networks**]: Distributed Systems—*Distributed applications*

General Terms: Human Factors, Management, Measurement

Additional Key Words and Phrases: Trust management, social networks, social trust, trust models

ACM Reference Format:
Sherchan, W., Nepal, S., and Paris, C. 2013. A Survey of trust in social networks. ACM Comput. Surv. 45, 4, Article 47 (August 2013), 33 pages.
DOI: http://dx.doi.org/10.1145/2501654.2501661

1. INTRODUCTION

The concept of social networks was first introduced by J.A. Barnes [1954], who describes them as connected graphs where nodes represent entities and edges their interdependencies. Entities could be individuals, groups, organizations, or government agencies. The edges could be interactions, invitations, trades, values, etc. In recent times, the emergence of Web-based social networks such as Myspace and Facebook has extended the notion of social networks in terms of their sizes [Golbeck 2007]. The public accessibility of Web-based social networks using mobile phones makes such platforms ubiquitous [Humphreys 2007]. Recent statistics by HitWise [Hanchard 2008] show that user retention rates of social networks are as good as online banking at high nineties,

Authors' addresses: W. Sherchan, IBM Research Australia, Australia; S. Nepal (corresponding author), C. Paris, CSIRO ICT Centre, Australia; email: Surya.Nepal@csiro.au.

DOI: http://dx.doi.org/10.1145/2501654.2501661

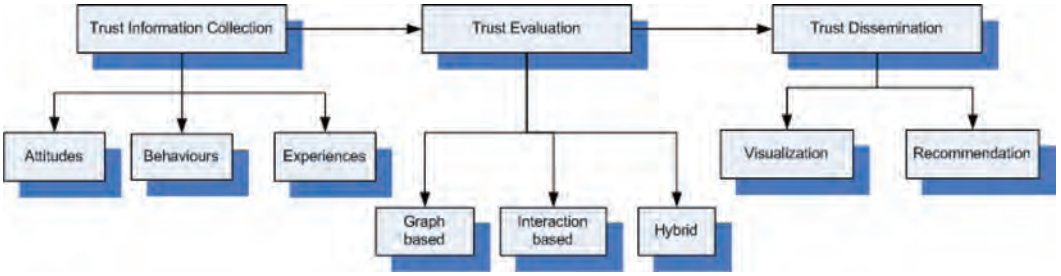

Fig. 1. Building a social trust system- classification.

suggesting that social networks are here to stay and remain a mainstream interaction platform for the foreseeable future.

The use of Web-based social networks was initially limited to connecting individuals to their friends and families [Haythornthwaite 2005]. The phenomenal growth of social network users in recent times has not gone unnoticed. Governments and enterprises have started exploiting the potential use of social networks as platforms for delivering and improving their services [Jaeger et al. 2007; Zappen et al. 2008]. However, there have been reports in the media of many incidents of breaching privacy of individuals through social networks [Gross and Acquisti 2005]. Given the open nature of Web-based social networks and their current level of popularity, users are increasingly concerned about privacy, an important consideration for them. In order to balance the open nature of social networks and safeguard the privacy concerns of users, it is important to build *trust communities*, which we define as communities that create an environment where members can share theirs thoughts, opinions, and experiences in an open and honest way without concerns about privacy and fear of being judged. These communities are built on authenticity, open sharing, like-mindedness and mutual respect. We contend that *social trust* provides an ideal foundation for building trust communities. Therefore, *trust* becomes an important aspect of social networks and online communities.

Trust has been studied in many disciplines including sociology [Helbing 1994; Mollering 2002; Molm et al. 2000], psychology [Rotter 1967; Cook et al. 2005], economics [Granovetter 1985; Huang 2007], and computer science [Maheswaran et al. 2007; Hughes et al. 2005]. Each of these disciplines has defined and considered trust from different perspectives, and their definitions may not be directly applicable to social networks. In general, trust is a measure of confidence that an entity or entities will behave in an expected manner. In this article, we review the definitions and measurements of trust from the prism of different disciplines, with a focus on social networks. The most important asset of any society or a social network is its *social capital* [Nahapiet and Ghoshal 1998; Moibus and Quoc-Anh 2004]. We consider the richness of the interactions between members in the social network as its social capital. In the context of social networks, trust is derived from social capital, which we call *social trust*.

In general, trust literature can be categorized based on three criteria: (i) trust information collection, (ii) trust value assessment, and (iii) trust value dissemination as shown in Figure 1. Each in turn can be further classified: trust information collection into three sources, namely (i) attitudes, (ii) behaviors, and (iii) experiences; trust value assessment according to the data model, namely (i) graph, (ii) interaction, and (iii) hybrid; and trust value dissemination into trust-based recommendation and visualization models. This article uses this categorization and classification scheme to review the literature.

The rest of the article is organized as follows. Section 2 provides a summary of existing related survey articles. Section 3 gives a brief review of trust definitions,

trust types, properties, and measurement models from the perspective of different disciplines. Section 4 discusses social networks and their properties and outlines the importance of trust in social networks. Section 5 first presents a definition of *social trust*, and then compares it to social capital. Sections 6, 7, and 8 review the literature under three different categories: trust information collection models, trust evaluation models and trust dissemination models, respectively. These reviews focus specifically on trust in the context of social networks. Section 9 presents a comparison of trust literature using the classification criteria defined in Figure 1, and then identifies the issues requiring further research. The last section concludes the survey.

2. PREVIOUS REVIEWS

Given the fact that trust is a multidisciplinary concept and has been around before the electronic age, it is a well-studied area from different disciplines. It is thus not surprising that there are already some review articles on different aspects of trust. This section aims to present a summary of existing review articles on trust and reputation and positions this article. In this article, we refer to both trust systems and reputation systems as trust systems since most reputation systems in the literature are developed for assessment of trust.

We categorize the existing review articles in two broad categories from the point of view of applications: network applications, in particular, peer-to-peer (P2P) applications, and Internet applications. Azer et al. [2008] survey trust and reputation schemes for ad hoc networks, focusing on the goals, features, and architectures of the trust management system for such networks. Momani and Challa [2010] review the treatment of trust in various network domains, more specifically wireless and sensor network domains. Finally, Suryanarayana and Taylor [2004] review trust management in P2P applications, classifying it into three broad categories: credential and policy based, reputation based, and social network based. The basic idea behind the credential- and policy-based trust management is to use credentials to enable a policy-based access control of the resources. This method is useful when there is an assumption of implicit trust on the resource owner. The reputation based trust management system, in contrast, provides an ability to evaluate the trust of the resource owner based on reputation values. The social-network-based method uses social relationships to rank nodes in the network. Suryanarayana and Taylor's review is limited to three different social-network-based methods of evaluating trust: community-based reputation [Yu and Singh 2000], regret [Sabater and Sierra 2002], and node ranking [Sabater and Sierra 2002].

In Internet applications, trust has been studied from three different aspects: Web site content, Web application, and its services. Beatty et al. [2011] conduct a metastudy of consumer trust on e-commerce Web sites, focusing on the organization of the Web site contents to ensure trustworthiness. In their work, Grandison and Sloman [2000] survey trust from the point of view of applications to identify trust needs for e-commerce applications and provide a comprehensive set of features required for developing a trust management system. The semantic Web has recently gained popularity for the development of Web sites and applications, and some work has addressed issues of trust in the semantic Web; see Artz and Gil [2007] for an overview of trust research in the semantic Web from the computer science perspective. In recent times, trust has also been widely studied in the area of service computing [Malik et al. 2009; Chang et al. 2006], where trust plays a major role in selecting the best services for a user. Wang and Vassileva [2007] present a systematic review of various trust and reputation systems for Web service selection and propose a typology to classify them along three dimensions: centralized versus decentralized, persons/agents versus resources, and global versus personalized. Finally, Josang et al. [2007] publish an important survey for Internet

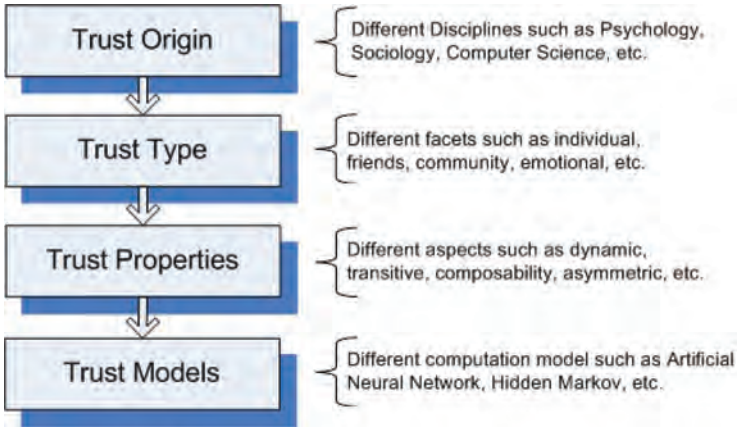

Fig. 2. Trust definitions and measurements.

applications in which they provide an overview of existing and proposed systems that can be used to derive measures of trust and reputation for Internet transactions.

In addition to the two broad categories described earlier, there are some general survey articles for trust. Foxample, Ruohomaa and Kutvonen [2005] survey trust management in general, providing an overview on three aspects of trust: the concept of trust management, trust management models, and trust information models. Their survey mainly focuses on trust initialization and the evolution of trust in trust management systems. Golbeck [2006b] reviews trust in Web content (including Web pages, Web sites, and semantic Web data), services (in P2P networks and Web services), and applications.

Some trust literature reviews have focused on one important aspect of trust: robustness against attacks. Hoffman et al. [2009] focus on attacks and defense mechanisms in reputation systems, categorizing attacks as: self-promoting, whitewashing, slandering, orchestrated, and denial of service. Kerr and Chon [2009] implement a number of cheating strategies against a few established trust systems, demonstrating that all of the tested trust systems are vulnerable to at least one type of premeditated attack from dishonest participants. Josang and Goldbeck [2009] discuss nine different types of attacks on trust and reputation systems, identifying the need for either a standard set of metrics for measuring the robustness of a trust system or some standard techniques for the theoretical robustness analysis of trust systems.

These review articles focus mainly on trust from a computer science perspective and do not consider relevant work in social sciences, mostly because current trust models tend to be driven by applications, and most of the network and Internet applications are developed and studied within computer science. The emergence of social networks has spurred new research in the study of trust, and, recently, a number of trust models for social networks have been developed with a specific focus on social aspects of trust. The aim of this article is to present a comprehensive review of trust in social networks covering both computer science and social sciences.

3. TRUST: DEFINITIONS AND MEASUREMENT

Trust is widely accepted as a major component of human social relationships. In general, trust is a measure of confidence that an entity will behave in an expected manner, despite the lack of ability to monitor or control the environment in which it operates [Singh and Bawa 2007]. Figure 2 shows that trust originated in different disciplines, leading to different types or facets of trust with different properties which

require different models. We organize this section accordingly. We first discuss trust definitions in the primary disciplines concerned with trust relationships: psychology, sociology, and computer science, followed by the various types of trust implied by these definitions. Then we describe the properties of trust and the existing models from the literature.

3.1. Definitions

Trust in Psychology. In psychology, trust is considered to be a psychological state of the individual, where the trustor risks being vulnerable to the trustee based on positive expectations of the trustee's intentions or behavior [Rotter 1967; Tyler 1990; Rousseau et al. 1998]. Trust is considered to have three aspects: cognitive, emotive, and behavioral [Beatty et al. 2011].

Trust in Sociology. In sociology, trust is defined as "a bet about the future contingent actions of the trustee" [Dumouchel 2005; Sztompka 1999]. This bet, or expectation, is considered to be trust only if it has some consequence upon the action of the person who makes the bet (i.e., trustor). Trust is considered from two viewpoints: individual and societal. At individual level, similar to the perspective from psychology, the vulnerability of the trustor is a major factor [Rousseau et al. 1998; Molm et al. 2000; Cook et al. 2005]. Trust is differentiated from cooperation in the presence of *assurance* (a third party overseeing the interaction and providing sanctions in case of misbehavior). However, cooperation in the presence of the shadow of the future (i.e., fear of future actions by the other party) is considered to be trust [Molm et al. 2000; Cook et al. 2005]. In this respect, social trust has only two facets, cognitive and behavioral, with the emotive aspect building over time as trust increases between two individuals [Kollock 1994; Lawler and Yoon 1996].

At societal level, trust is considered to be a property of social groups and is represented by a collective psychological state of the group. Social trust implies that members of a social group act according to the expectation that other members of the group are also trustworthy [Lewis and Weigert 1985] and expect trust from other group members. Thus, at societal level, social trust also has the institutional or system aspect of trust.

Trust in Computer Science. Trust in computer science in general can be classified into two broad categories: "user" and "system". The notion of "user" trust is derived from psychology and sociology [Marsh 1994], with a standard definition as "a subjective expectation an entity has about another's future behavior" [Mui 2003]. This implies that trust is inherently personalized. In online systems such as eBay and Amazon, trust is based on the feedback on past interactions between members [Resnick et al. 2000; Ruohomaa et al. 2007]. In this sense, trust is relational. As two members interact with each other frequently, their relationship strengthens, and trust evolves based on their experience. Trust increases between members if the experience is positive and decreases otherwise. In online systems, trust is considered to be of two types: direct trust and recommendation trust. Direct trust is based on the direct experience of the member with the other party. Recommendation trust is based on experiences of other members in the social network with the other party. Recommendation trust is based on the propagative property of trust. In P2P-based trust models, members gather information about other members using their social networks, sometimes also referred to as *referral networks* [Abdul-Rahman and Hailes 2000; Kautz et al. 1997]. Each peer models other peers in two ways: their trustworthiness as interaction partners (capability to provide services), called *expertise* in Singh et al. [2001], and their trustworthiness as recommenders (capability to provide good recommendations), referred to as *sociability* in Singh et al. [2001]. After each interaction in the environment, the expertise of the interaction partner and the sociability of the peers in the referral chain that led to the interaction are updated to reflect the experience of the member in that

interaction. The immediate neighbors of the member are also periodically updated to reflect the change(s) in the evaluated trust of those members. This is influenced by both the neighbor's expertise and sociability. Marmol and Perez [2011] present a comparison of several computational trust models such as EigenTrust [Kamvar et al. 2003], PowerTrust [Zhou and Hwang 2007], and PeerTrust [Xiong and Liu 2004].

The standard notion of "system" trust, derived from the security domain [Yao et al. 2010], is "the expectation that a device or system will faithfully behave in a particular manner to fulfil its intended purpose". For example, a computer is trustworthy if its software and hardware can be depended on to perform as expected, such that its services are still available today, unaltered, and behave in exactly the same way as they did yesterday [Moreland et al. 2010]. The notion of "system" trust is supported by both software- and hardware-based solutions. For example, Seshadri et al. [2004] presented a software-based mechanism, while Chen and Li [2010] described a hardware-based mechanism. "System" trust is out of the scope of this survey. We note, however, the work of the Trusted Computing Group (TCG), which includes a Trusted Platform Module (TPM), a cryptographic microcontroller system that enables the TPM to be a root of trust for validating both the hardware and software characteristics of a remote computer on which the TPM is installed [Challener et al. 2007; Nepal et al. 2010b]. See also Moreland et al. [2010] for a good review of technologies in the context of a personal trusted device.

Across all the disciplines, two important aspects characterize a trust relationship: *risk* and *interdependence* [Rotter 1967; Coleman 1990; Williamson 1993]. The source of risk is the uncertainty regarding the intention of the other party. Interdependence is characterized by the fact that the interests of the two parties are related and cannot be achieved without relying on each other. The relationship is not a trust relationship if these two conditions do not exist. Since risk and interdependence are necessary conditions for trust, changes in these factors over the course of a relationship may alter both the level and the form of that trust [Rousseau et al. 1998].

3.2. Types/Facets of Trust

We now discuss the different facets of trust from the various disciplines.

Calculative. The calculative aspect of trust defines trust as the result of a calculation on behalf of the trustor designed to maximize the trustor's stakes in the interaction [Tyler and Degoey 1996]. This aspect of trust is prevalent in economics, where the prisoner's dilemma games are used to model trust and cooperation. It is also common in organizational science. Coleman [1990] describes this phenomenon as: "A rational actor will place trust . . . if the ratio of the chance of gain to the chance of loss is greater than the ratio of the amount of the potential loss to the amount of the potential gain."

Relational. The relational aspect of trust defines trust built up over time as a result of repeated interactions between the trustor and trustee. Information available to the trustor from within the relationship itself forms the basis of relational trust. Reliability and dependability in previous interactions with the trustee give rise to positive expectations about the trustee's intentions [Rousseau et al. 1998]. In computer science, this aspect of trust is termed direct trust (trust based on direct interactions between two parties).

Scully and Preuss [1996] study the relationship between calculative trust and relational trust in an organization in the context of work transformation. They find that, for employees working in the traditional context of narrow, individualized tasks, calculative trust plays a greater role than relational trust in making a decision to take up courses supporting work transformation. In contrast, for employees working in team-based environments, the decision is based on relational trust (of the team mates) rather than calculative trust; (i.e., individual gain).

Emotional. The emotional aspect of trust defines the security and comfort in relying on a trustee [Kuan and Bock 2005]. In psychology, emotional trust is perceived to be an outcome of direct interpersonal relationships [Holmes 1991]. Emotional trust influences the trustor to form positive perceptions of the relationship continuity and is affected by cognitive trust. Empirical studies such as Taylor [2000] show that the trustor's previous direct experiences can affect his/her emotions and hence his/her emotional trust on the trustee. Holmes et al. [1991] likens emotional trust to an emotional security which enables someone to go beyond the available evidence and feel assured and comfortable about relying on a trustee.

Cognitive. The cognitive aspect of trust is defined as trust based on reason and rational behavior [Lewis and Weigert 1985; Kuan and Bock 2005]. According to the social capital theory [Coleman 1988], three forms of social capital can affect cognitive trust: information channels, norms and sanctions, and the trustee's obligations to the trustor. Additionally, the social relation structures within networks and the strength of the ties between members can impact the trustor's cognitive trust of the trustee [Granovetter 1973]. Specifically, positive referrals within the relations of social networks increase cognitive trust in the trustee [Komiak and Benbasat 2004; Kuan and Bock 2005]. Mollering [2002] suggests that cognitive trust precedes emotional trust, and that emotional trust leads to the formation of favorable or unfavorable expectations of the trustee.

Institutional. The institutional trust is trust as a result of an institution providing an environment that encourages cooperation between members and penalizes misbehaviors [Lewis and Weigert 1985]. Such supports can exist at organizational level [Miles and Creed 1995] and at societal level such as legal systems that protect individual rights and property [Fukuyama 1995]. Publius [Waldman et al. 2000] is an example of an application that uses institutional trust to allow users to publish materials anonymously such that censorship of and tampering with any publication in the system is very difficult.

Dispositional. This aspect of trust recognizes that, over the course of their lives, people develop generalized expectations about the trustworthiness of other people [Rotter 1967, 1971. This is embodied in dispositional trust, which is extended to everyone regardless of whether the trustor has knowledge of the trustworthiness about the trustee or not. Cooperative tendency [Huang 2007], a form of social capital, and genetic predisposition [Sturgis et al. 2010] can be considered to contribute to dispositional trust.

Figure 3 shows three types of trust relationships in an online social network: (a) trust between members of the network, (b) trust between a member and the provided online service, and (c) trust between a member and the service provider. We have so far discussed the different facets for the first type of trust relationship, which is the main focus of this article. There have also been some studies on the other two types of trust relationships.

The trust that exists between a member and the service provided depends on many factors, including the service interface design [Wang and Lu 2010]. For example, in the context of Internet banking, Suh and Han [2002] showed that a customer's perceived ease of use of an interface has a positive impact on his/her perceived usefulness of the system, which in turn has a positive impact on his/her trust in Internet banking. This means the ease of use of social networking sites enhances members' trust in them.

The trust relationship between members and service providers has been studied in the field of business and marketing. For example, Johnson and Grayson [2005] have found that service providers' expertise and service performance lead to cognitive trust. From their study, they defined a model of customer trust in service providers based on cognitive and affective trust.

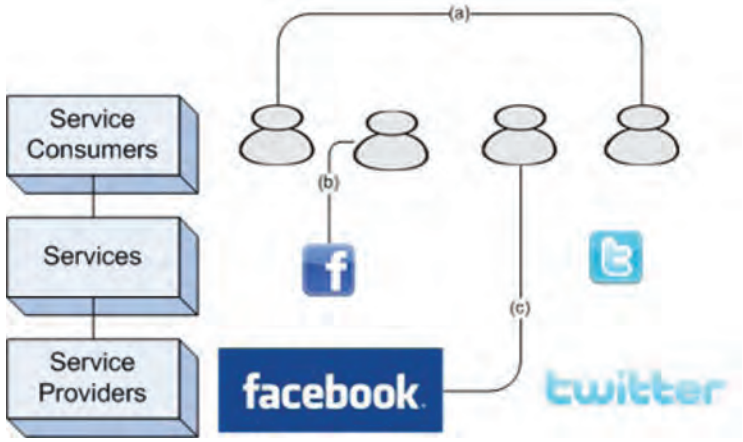

Fig. 3. Trust relationships in an online social network.

The trust relationship of a member with the mediation system on mediated online social networks is defined by both the trust between a member and the service provided and a member and the service provider. Coulter [2002] finds that the relationship between a member and a provided service is moderated by the length of the relationships between the member and the service provider. McLeod and Pippin [2009] study the trust relationships between a member, the service provided, and a service provider in the context of eGovernment. They classify them into two broad categories: system trust, which includes security, privacy, and all the logic aspects, and relationship trust, which includes associated entities and software.

3.3. Properties of Trust

Context specific. Trust is context specific in its scope. For example, Mike trusts John as his doctor, but he does not trust John as a mechanic to fix his car. So John is trustworthy in the context of seeing a doctor, but he is not in the context of fixing a car. This is different from *trust context*, which normally refers to the environment in which the trust relationship exists, for example, law enforcement, insurance, and social control [Toivonen et al. 2006]. The context-specific nature of trust is discussed in social and psychological sciences [Rousseau et al. 1998].

Dynamic. Trust can increase or decrease with new experiences (interactions or observations) [Staab et al. 2004]. It may also decay with time. New experiences are more important than old ones, since old experiences may become obsolete or irrelevant with time. This property of trust is extensively modeled in computer science. Various techniques are used for modeling this dynamicity, for example, aging of old interactions in Wishart et al. [2005], Kamvar et al. [2003], and von Laszewski et al. [2005], giving more weight to recent interactions in Song et al. [2005], and Zhang and Fang [2007] and using only the most recent interaction in Jurca and Faltings [2003]. In some models, such as PeerTrust [Xiong and Liu 2003, 2004], users are allowed to choose the temporal window for dynamic aging of old interactions/experiences as per their need. In others, such as PowerTrust [Zhou and Hwang 2007], trust computation is performed periodically to ensure that the computed trust values are up-to-date.

Propagative. Trust is propagative, in that if Alice trusts Bob, who in turn trusts John, whom Alice does not know, Alice can derive some amount of trust on John based on how much she trusts Bob and how much Bob trusts John. This is not to say, however, that trust is transitive. Because of its propagative nature, trust information can be

passed from one member to another in a social network, creating trust chains. It is the propagative property of trust that is being used in Josang et al. [2003], where a recommendation system is used to allow trust propagation according to explicit conditions. Propagation of trust along social network chains is similar to the "word of mouth" propagation of information for humans [Abdul-Rahman and Hailes 2000]. Propagation is the most studied property of trust. Various trust models [Schillo et al. 2000; Mui et al. 2002; Sabater 2002; Yu et al. 2004] have used this property. Similarly, literature based on the FOAF (Friend-Of-A-Friend)[1] topology are all based on the propagative nature of trust.

Non-transitive. Generally, trust is *not* transitive [Christianson and Harbison 1996; Yu and Singh 2000]. If Alice trusts Bob and Bob trusts John, this does not imply that Alice trusts John. Transitivity implies propagation, but the reverse is not true. Unfortunately, the propagative nature of trust is sometimes confused with the transitive nature of trust in the literature, for example, Josang et al. [2003].

Composable. Propagation of trust and distrust along social chains allows a member to form some trust on a member not directly connected to her. However, when several chains recommend different amount of trust for a member, then the trustor needs to compose the trust information. For example, Bob is recommended to Alice by several chains in her network. In this case, Alice needs to compose the trust information received from different chains to decide whether she can trust Bob. This is potentially difficult if the information is contradictory. The composability of trust provides another way of computing trust in social networks [Golbeck 2005b]. Richardson et al. [2003] use the concept of an openly defined composition function to evaluate trust based on composability of trust. Golbeck [2005b] proposes a trust composition function based on the structure of trust relationships. Typically, models that employ propagation feature of trust also employ the composition feature to utilize propagated trust values from several trust chains in making trust decisions, for example, Zuo et al. [2009].

Subjective. In general, trust is subjective. For example, Bob gives an opinion about a movie. If Alice thinks Bob's opinions are always good, she will trust Bob's review. However, John may think differently about Bob's opinions and may not trust the review. The subjective nature of trust leads to personalization of trust computation, where the biases and preferences of the trustor have a direct impact on the computed trust value. Various trust models consider personalization of trust [Walter et al. 2009; Sabater and Sierra 2005; Wang and Vassileva 2007]. Jackson [1999] stresses the importance of personalized trust in social and organizational relations. In computer science, personalized trust has been studied in Zacharia and Maes [2000], Sabater [2002], and Yu et al. [2004] among others. Based on sociological studies of human behavior [Granovetter 1985; Castelfranchi et al. 1998], Mui et al. [2002] argue that a person is likely to have different levels of trust in the eyes of others, relative to the embedded social network.

Asymmetric. Trust is typically asymmetric. A member may trust another member more than s/he is trusted back. However, when both parties are trustworthy, they will converge to high mutual trust after repeated interactions. Conversely, if one of the members does not act in a trustworthy manner, the other member will be forced to penalize him/her, leading to low mutual trust. Asymmetry can be considered a special case of personalization. Asymmetry occurs because of differences in peoples' perceptions, opinions, beliefs, and expectations. The asymmetric nature of trust has been identified in various hierarchies within organizations [Yaniv and Kleinberger 2000].

Self-reinforcing. Trust is self-reinforcing. Members act positively with other members whom they trust. Similarly, if the trust between two members is below some threshold,

[1]http://www.foaf-project.org/.

it is highly unlikely that they will interact with each other, leading to even less trust on each other [Yu and Singh 2000]. This aspect of trust has received comparatively less attention in the literature.

Event sensitive. Trust takes a long time to build, but a single high-impact event may destroy it completely [Nepal et al. 2010a]. This aspect of trust has received even less attention in computer science.

3.4. Trust Models

Various trust models have been proposed in the literature. The techniques used can be broadly classified into statistical and machine learning techniques, heuristics-based techniques, and behavior-based techniques. Statistical and machine learning techniques focus on providing a sound mathematical model for trust management. Heuristics-based techniques focus on defining a practical model for implementing robust trust systems. Behavior-based models focus on user behavior in the community.

Bayesian systems [Mui et al. 2002; Josang and Ismail 2002] and belief models [Josang 2001; Yu and Singh 2002; Josang et al. 2006] are the major examples of purely statistical techniques. Typically, in Bayesian systems, binary ratings (honest or dishonest) are used to assess trust by statistically updating the beta probability density functions. In a belief model, a consumer's belief regarding the truth of a rating statement is also factored into the trust computation. The techniques for combining beliefs vary. For example, Dempster-Shafer theory is employed in Yu and Singh [2002], while subjective logic is used in Josang [2001] and Josang et al. [2006]. Solutions based on machine learning typically exploit techniques such as Artificial Neural Networks (ANNs) and Hidden Markov Models (HMMs) for computing and predicting trust. For example, Song et al. [2004] use HMM for evaluating recommender trust, and ElSalamouny et al. [2010] propose a discrete HMM-based trust model. Since both statistical solutions and machine learning solutions are highly complex, researchers have moved towards heuristics-based solutions. These solutions, such as Xiong and Liu [2004] and Huynh et al. [2006], aim to define a practical, robust and easy to understand and construct trust management system. Malik et al. [2009] present a hybrid solution defining key heuristics and a statistical model (HMM) for reputation assessment.

Adali et al. [2010] present a behavior-based model, where trust is evaluated based on the communication behavior of members in a social network. Behavioral trust is evaluated based on two types of trust: conversation trust and propagation trust. Conversation trust specifies how long and how frequently two members communicate with each other. Longer and more frequent communication indicates more trust between the two parties. Propagation trust refers to the propagation of information. Propagating information obtained from one member to various other members indicates that a high degree of trust is being placed on the information and, implicitly, its source.

4. SOCIAL NETWORKS

As mentioned in the Introduction, a social network is described as a social structure made of nodes connected by edges that represent one or more specific types of interdependency [Barnes 1954]. Nodes represent individuals, groups, or organizations, while the connecting edges are relations like values, ideas, friendship, trade, etc. Figure 4 shows an example social network, looking at a specific person: Alice. The nodes represent people, the edges relationships amongst them. This specific network depicts Alice's relationships with different people. Still focused on Alice, a different social network could be constructed for depicting her interests and hobbies (nodes in that case would include interests and hobbies). These two networks could in fact be combined to depict both information in one network.

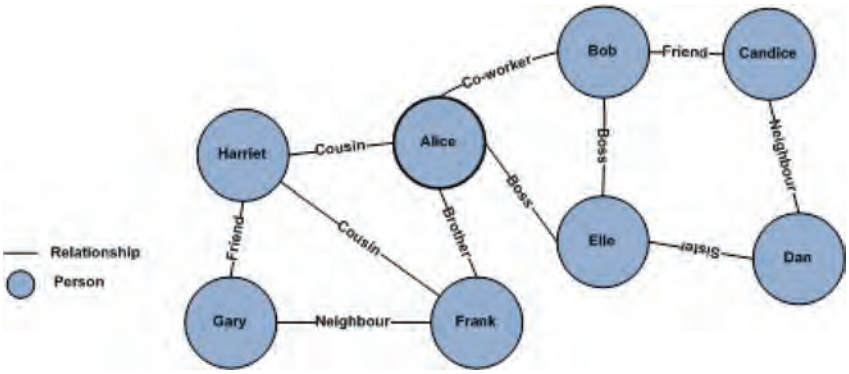

Fig. 4. An example social network.

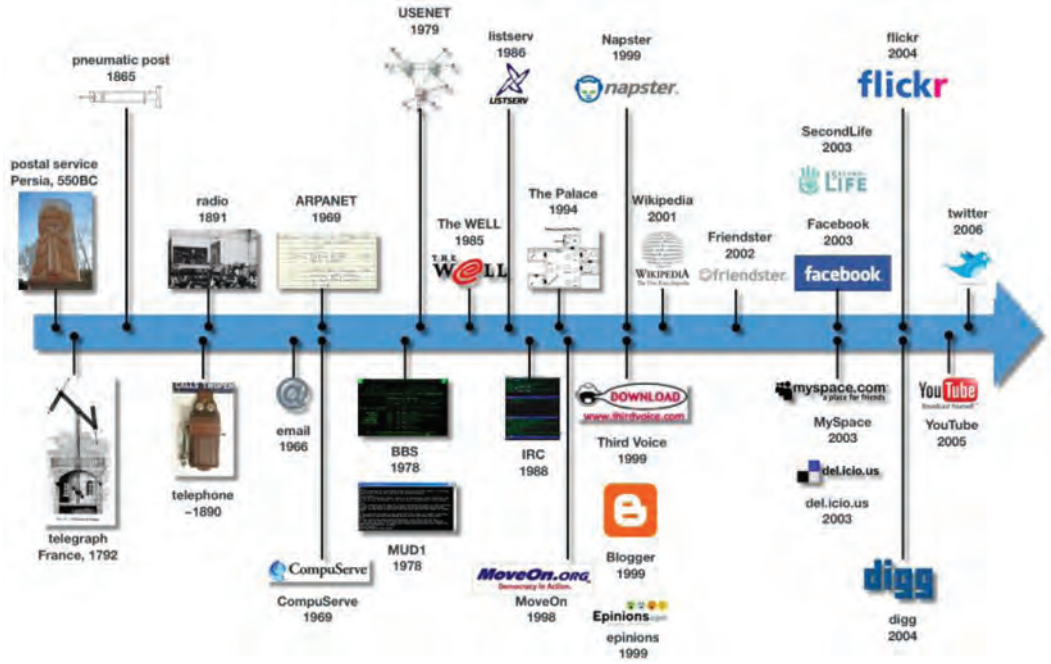

Fig. 5. Evolution of social media and social networks.

Social networks can be used for analyzing complex relationships in a variety of disciplines, including anthropology, biology, communication studies, economics, geography, information science, organizational studies, social psychology, and sociolinguistics. The concept of social networks has evolved over the years, and now social network analysis is a paradigm with its own theoretical statements, methods, software, and researchers. Studies have been done on different aspects of social networks and how they are affected by external factors. With the evolution of technology, Web-based social networks have proliferated (see Figure 5[2]). Currently there are hundreds of social networking

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

sites operational in the World Wide Web. We next discuss issues raised by technological advances to research in social networks and social network analysis.

Wellman [2004] explores the advent of the Internet and its effect on social connections. In the early days of the Internet, there were two conflicting views. The utopian view considered that the Internet would significantly enhance social connections and create opportunities for new connections, thereby extending one's social network. In contrast, the dystopian view was that connections formed via the Internet were not real nor authentic; therefore, the Internet would serve to further alienate people from their community and society. Studies conducted over the years show that neither of these views has merit. Over the years, the Internet has become part of people's lives. It has not diminished social connections but has enhanced them with frequent communication. It has served to maintain strong connections and make weak connections stronger. Online-only connections are not common. People who first interact via online medium often find ways to connect in the real world. In this respect, the Internet/online world is part of the real world. The Internet is becoming another means of communication integrated into the regular patterns of social life. It has fostered "individual connectivity", that is, the Internet and new communication technologies are helping people to personalize their own communities. This is neither a dystopian loss of community nor a utopian gain, but rather a complex, fundamental transformation in the nature of community from groups to social networks.

Wellman [1996] shows how social network analysis might be useful for understanding how people relate to each other through computer-mediated communication. Similar to real-life social networks, Computer-Supported Social Networks (CSSNs) provide a basis for social support. CSSNs encourage both specialized and multiplex relationships and also result in strong ties in relationships between participants. Social networks are of two types: (i) densely knit social networks, in which members have frequent communication and are tightly bounded, and (ii) sparsely knit, loosely bounded networks, where only few members have frequent and direct communication with each other. Computer networks support both types of social networks. Wellman [1996] shows that CSSNs successfully help maintain strong, supportive ties of work and community, and they foster an increase in the number and diversity of weak ties. They are especially suited to maintaining intermediate-strength ties between people who cannot see each other frequently. Online relationships are based more on shared interests and less on shared social characteristics. Although many relationships function offline as well as online, CSSNs are developing norms and structures of their own. CSSNs have given rise to the now popular Web-based social networks as can be seen in Figure 5.

In this section, we first discuss properties of social networks as defined in various disciplines; then, we discuss the importance of trust in these networks.

4.1. Properties of Social Networks

Homophily. Sociologists, [McPherson et al. 2001] analyze hundreds of studies of homophily in social networks. Homophily is the tendency of individuals to associate and bond with similar others, which means that people's personal networks tend to be homogeneous with regard to many socio-demographic, behavioral, and intra-personal characteristics. Homophily limits people's social worlds in a way that has powerful implications for the information they receive, the attitudes they form, and the interactions they experience. In their work, McPherson et al. review different types of network relationships that are considered homophilous, the different dimensions on which similarity induces homophily, the sources of homophily, that is, social structures that induce propinquity among similar others, and the cognitive processes that make communication between similar others more likely. They also identify that the patterns of homophily tend to grow stronger if two people are connected by multiple forms

of relationship. Homophily are of two types [Lazarsfeld and Merton 1954]: (i) status homophily, based on ascribed status such as race, ethnicity, age, religion, education, occupation, etc., which means that individuals with similar social status characteristics are more likely to associate with each other, and (ii) value homophily, based on values, attitudes, and beliefs, that is, a tendency to associate with others who think in similar ways, regardless of differences in status. Homophily in social networks is analogous to the phenomenon of "echo chamber" in media [Jamieson and Cappella 2009].

Small-world phenomenon. There are two different views on the "small world" phenomenon in social networks. Milgram, the original developer of the "small-world problem", famously identified "six degrees of separation" between any two people in the world [Milgram 1967]. Watts [2003] later investigated the "small-world problem" in the modern computerized world, where small world networks were assumed to be everywhere (e.g., online social networks; email networks; networks of movie stars, boards of directors, and scientists; neural networks; genetic regulatory networks, protein interaction networks, metabolic reaction networks; World Wide Web; food Webs; etc.). Although the study suffered very low chain completion rates, the average length of completed chain (4) corresponded to Milgram's study (6). These works view our world as a "small world", where everyone is connected to each other with a small chain of average 6 people in-between. Another view is that instead of being one highly connected small world, our world consists of many loosely connected and some disconnected small worlds. Kleinfeld [2002] reviews several studies conducted on the "small world problem" and its variations. He reveals low chain completion rates in almost all of the experiments, suggesting that a vast majority of people in the world are very disconnected, contrary to the believers of "small world". In addition, one recurring conclusion in these studies is that connections are weak outside racial, socio-economic, and geographic boundaries. This reinforces the homophilous nature of social networks that allows creation of these numerous small worlds.

4.2. Importance of Trust in Social Networks

Web-based social networks are a special form of social networks that have grown in numbers and scope since the mid 1990s [Golbeck 2005b]. Web-based social networking has given rise to numerous online communities and has become a mainstream communication medium for individuals and organizations [Golbeck 2007]. This is evident from the popularity of social networking sites such as Facebook[3] and MySpace[4] for creating personal and commercial pages. This popularity has been a driving force for generating a large number of social networks on the Web targeting specific communities of interest. Social networking sites provide a forum for their members to connect with other members in the networks and share hobbies, opinions, and life experiences, including daily activities. Many of these social networking sites are built with the aim of connecting as many people as possible.

The concept of FOAF is prevalent in many social networks [Mika 2007]. The underlying assumption behind this concept is that the relation "friendship" is transitive. The foundation of every friendship is trust. Thus, the FOAF relationship indirectly implies that trust is also transitive in the social networks. However, as discussed earlier, trust is propagative, not transitive. We might trust someone, but may not be sure about his or her friends. Therefore, there is an inherent risk to the private data of the members in such social networks due to the underlying assumption of implicit trust in the FOAF relationship. Such dangers in social network sites have been experienced and exposed in recent times as reported in Dwyer et al. [2007] and Young and Quan-Haase

[3]http://www.facebook.com/.
[4]http://www.myspace.com/.

[2009]. The lack of trust in the social networks goes against their vision of connecting like-minded people, as members may not feel comfortable to express their opinions and share ideas. Users trusting each other, working, and interacting with each other is the real source of power and growth for any community. Therefore, trust becomes a critical factor in the success of these communities.

Another concept studied in social networks in the context of trust is tie strength and relationships. Granovetter [1973] introduces the concept of tie strength in relationships. Tie strength is characterized by time, emotional intensity, intimacy, and reciprocity. Strong ties indicate the circle of trusted people with whom one has already established a trusted relationship, whereas weak ties point to mere acquaintances. Gilbert and Karahalios [2009] apply the concept of tie strength to social media data, specifically to Facebook datasets, and map the friendships between members into strong or weak ties using binary modes, that is, the relationship is categorized as either strong or weak. However, in reality, a tie strength can fall anywhere along the spectrum from weak to strong. To address this issue, Xiang et al. [2010] propose an unsupervised method to infer a continuous-valued relationship strength in social networks. The concept of tie strength has been applied and studied for different applications such as transfer of knowledge [Levin et al. 2004]. Though it is not explicitly mentioned, tie strength is one of the important dimensions for understanding trust in social networks, as a strong tie implicitly defines the trust relationship. Deriving a trust model based on tie strength is an interesting area of future research.

Social trust computation has other applications as well. Golbeck [2006a] uses social trust and provenance information for semantic Web content filtering. Schneider [2009] employs social trust to improve security with the deployment of a distributed software system on top of an embedded platform. Zarghami et al. [2009] introduce a metric, the T-index, to estimate a user's trustworthiness for making recommendations. This index is similar to the h-index in the research community.

5. SOCIAL CAPITAL AND SOCIAL TRUST

In this section, we first define social capital and then differentiate between social capital and social trust. We follow with a discussion of how social trust can be derived from social capital. This provides the foundation for the reviews in the next three sections.

5.1. What is Social Capital?

There is no universal agreeable definition of social capital due to ideological reasons. Specific definitions of social capital are influenced by their discipline of origin (e.g., social science, political science, etc.) and the level of observation (e.g., at the individual or household level, at the group, community, or neighborhood level, at the regional or national level). A good introductory summary of social capital and a considerable number of definitions can be found in Claridge [2004]. As our focus is on social networks, we consider social capital from that perspective only.

Social capital refers to the collective value associated with a social network. Various approaches for measuring it have been proposed in the literature. Nahapiet and Ghoshal [1998] propose to measure social capital along three dimensions: structural (patterns of social interactions between actors), relational (the relationships between the actors), and cognitive (shared representations, interpretations, and systems of meaning among actors). Mobius and Quoc-Anh [2004] suggest that social capital could be defined as either preference based (directed altruism) or cooperative (repeated interactions between pairs or groups of actors). Brunie [2009] studies social capital through three dimensions: relational (ability of a member to mobilize social contacts in order to obtain valued resources), collective (resource to facilitate cooperation at group level), and generalized (values and attitudes that influence how people relate to each other

and that predispose them to cooperate, trust, understand, and empathize with each other). All these approaches are applicable to social networks. However, we follow Brunie's definition from the collective dimension as it considers social capital from the perspective of the whole community. Brunie [2009, page 255] defines the social capital from the collective perspective as follows.

> "... a collective resource that facilitates cooperation at the small group level.... no longer resides with an individual but exists through relationships between actors ... is based on the density of interactions ..."

It is clear from this definition that interactions play an important role in defining and measuring social capital. In an online community, social capital refers to the value derived from the interactions that provide support for bonding between like-minded people. We thus define the social capital of an online community as the density of interactions that is beneficial to the members of the community. Our definition is in line with Putnam's [2000] view that refers to social capital as a resource that can be drawn on by individuals through building up connections with others in social and community groups. Our definition has two important elements: (a) the number of interactions and (b) the nature of interactions. Social capital is low if the number of interactions among members is high, but the nature of these interactions is not beneficial to individuals.

5.2. Social Capital versus Social Trust

Social trust is considered an important aspect of social capital that represents the cooperative infrastructure of a society [Coleman 1988; Putnam 1995]. Social scientists focus on increasing social trust through investment in human capital [Huang 2007]. The distinctions between social capital and social trust have sometimes been blurred in the literature. For example, Paldam [2000] defines social capital as the quantity of trust a member has in other members in the society. This type of definition does not distinguish social capital from social trust. Social trust is an important element of social capital, but they are not the same. This distinction is clear in the publication of Putnam's work on Bowling Alone [Putnam 2000, 1995]. Putnam [1995, page 67] defines social capital as follows.

> "By analogy with notions of physical capital and human capital—tools and training that enhance individual productivity— 'social capital' refers to features of social organization such as networks, norms, and social trust that facilitate coordination and cooperation for mutual benefit."

This definition implies that social capital encompasses much more than social trust [Alesina and La Ferrara 2002]. According to Putnam's theory, there is a presence of social capital in the community when the members in the community exhibit good behavior. Good behavior is only possible if there is trust among the members. While not equivalent, social trust and social capital are interconnected in many ways and build on each other.

Huang [2007] examines the role of individual cooperative tendencies in generating social trust. He studies the relationship between social trust and human/social capital with a focus on how human capital could be cultivated to increase social trust. The work is based on the premise that individuals differ in their predisposition to cooperate. Some people are inherently more trusting than others, such as altruistic people who help others without calculating personal gain. Such people are referred to as having a "cooperative tendency". Cooperative tendency is considered to be a component of human capital that is costly to cultivate but yields a stream of returns in the future (especially in increasing social trust). When more people have higher cooperative tendencies in a

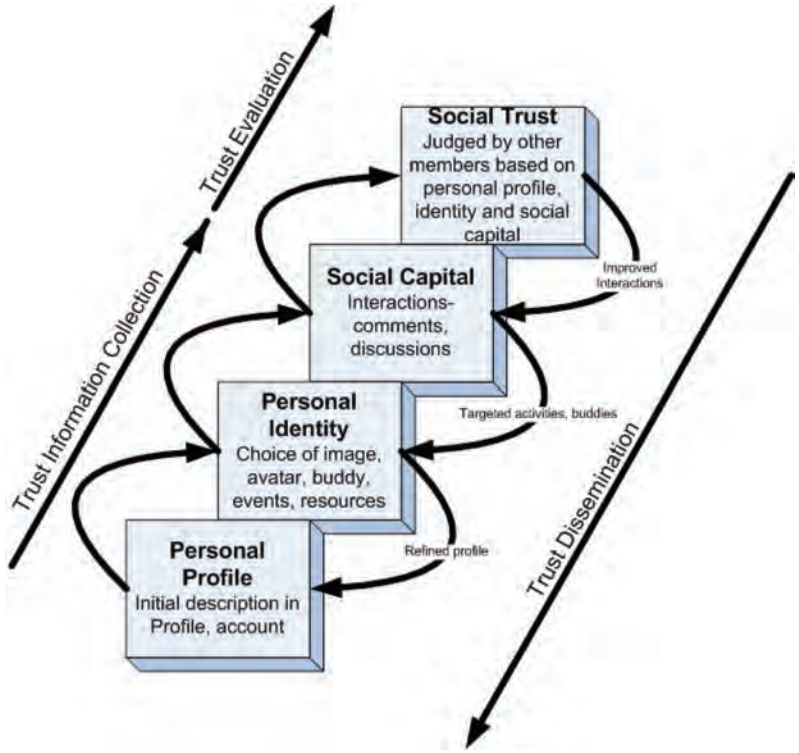

Fig. 6. Process of creating social trust.

society, they are more trusting, and hence the social trust of the society is higher. Based on the notion of cooperative tendencies, Huang [2007, page 554] writes:

> "... Social trust in a group is equal to the perceived trustworthiness of a typical member or the average trustworthiness of all members, characterized by the proportion of cooperative players in the group. The level of social trust is determined by the distribution of cooperative tendency in the group and the specific game features, which is why it varies across players and games ..."

Sturgis et al. [2010] study the possibility of genetic and environmental basis for social trust. They analyze data collected from samples of monozygotic and dizygotic twins to estimate the additive genetic, shared environmental, and nonshared environmental components of trust. The results show that the majority of the variance in a multi-item trust scale is accounted for by an additive genetic factor. The environmental influences experienced in common by sibling pairs have no discernible effect; the only environmental influences appear to be those that are unique to the individuals. This is in contrast to the common theories that development of social trust is influenced by social-developmental and political/institutional features of individuals and societies and can somehow be instituted in individuals in their early life (i.e., the view taken by works such as Huang [2007]).

5.3. Computing Social Trust from Social Capital

We capture the process of computing social trust from the social capital in an online community in Figure 6. The first step for a user in an online community is to create a

personal profile, after registering in the social network. This profile typically contains personal details the user would like to share with other members in the community (e.g., contact details, hobbies, etc.). The second step is to create a *personal identity*, through the choice of a screen name, an avatar/image, specific friends to invite, etc. The third step is to interact with other members of the community, thereby contributing to the *social capital*. Interactions could be in the form of providing information or providing comments on the information or comments on the other members' comments [Liu et al. 2008]. The last step is to compute the *social trust* from the social capital, which can in turn be used to improve the social capital of the network through recommendation systems [Chen and Chen 2001; Herlocker et al. 2000; Manikrao and Prabhakar 2005]. As shown in the figure, deriving social trust can be seen as consisting of three steps: (i) trust information collection, (ii) trust evaluation, and (iii) trust dissemination. We now review the literature from the perspective of these aspects.

6. TRUST INFORMATION COLLECTION MODELS

In social networks, trust information can be collected from three main sources: (i) attitudes, (ii) behaviors, and (iii) experiences.

Attitudes. Attitude represents an individual's degree of like or dislike for something. Attitudes are generally positive or negative views of a person, place, thing, or event. People can be conflicted or ambivalent toward an object, meaning they can simultaneously possess both positive and negative attitudes toward the item in question. Attitudes are judgements developed on the affect, behavior, and cognition model. An affective response is an emotional response that expresses an individual's degree of preference for an entity. A behavioral intention is a typical behavioral tendency of an individual. A cognitive response is a cognitive evaluation of the entity that constitutes an individual's beliefs about the object. Most attitudes are the result of either direct experience or observational learning from the environment. Unlike personality, attitudes can change as a result of experience. Jones [1996] argues that trust is a form of affective attitude. Dohmen et al. [2006] report from a survey that attitudes are transmitted from parents to children, indicating that attitudes can represent the dispositional aspect of trust.

The attitude information is derived from a user's interactions. For example, a user expresses a positive/negative view towards an activity, a service, or a process during an interaction with another member in the community. Such attitude information is typically captured using Likert-type scales [Likert 1932]. Helbing [1992] develops Boltzmann[5]-like mathematical models for attitude formation in social networks. Relatively little research effort has been focused on using attitude information to derive trust. This thus remains an important area for future research.

Experiences. Experiences describe the perception of the members in their interactions with each other. Experience information can be implicit or explicit. Explicit experiences are direct first-hand interactions with another member. Feedback mechanisms are tools for reflection on direct user experiences. Experiences may affect attitudes or behaviors. Positive experiences encourage members to interact frequently in the community, leading to a change in behavior. They may also lead to changes in attitudes and make the member more receptive towards similar information.

In computer science, a number of experience-based trust management frameworks have been proposed, for example, Klos and La Poutré [2005], Yang et al. [2007], and Wang et al. [2007]. Most of these trust models, such as PowerTrust [Zhou and Hwang 2007] and PeerTrust [Xiong and Liu 2004], are based on feedback. The feedback

[5] [Boltzmann 1964].

mechanism is specifically designed to capture a member's experience interacting with the other member. Reviews such as Mui [2003], Sabater and Sierra [2005], and Josang et al. [2007] discuss trust models ranging from Bayesian networks to belief models, all based on user feedback/experiences. Paradesi et al. [2009] present an integrated trust model for Web service composition. This model progressively updates the belief of users of a particular Web service when the feedback is available. However, the foundation of this model is users' feedback/experience rather than their behavior. All reputation based trust management models utilize user experience as the main source of trust information. Experiences provide one aspect of trust information in social networks and need to be considered along with the other aspects, namely, attitudes and behaviors.

Behaviors. Behaviors are identified by patterns of interactions. For example, if a member is a highly active participant and suddenly stops participating, this change in behavior is noticeable and might imply that this member's trust of the community or with the member(s) with whom he/she had been frequently interacting with has decreased. Findings and observations on behavioral aspects of users have been widely reported in Psychology, social science, behavior science and design systems, for example, Zajonc [1980] and Romer [2000]. The behavior of individuals in a society reflects much more about them than simply their past experience. Therefore, user behaviors provide an interesting aspect to trust in online communities.

Helbing [1994] proposes Boltzmann-like mathematical models for attitude formation and individual behaviors in social networks. Caverlee et al. [2008] propose tracking user behavior over time to encourage long-term good behavior and penalize bad/misbehavior in social networks. Based on the results of a survey, Yan et al. [2008, 2009] propose a trust model based on usage behaviors for mobile applications. The model assumes that users' perception leads to their intention, which results in their behavior. Nepal et al. [2010a] also make this assumption in their work, in which they use a Boltzmann-like equation for capturing the effect of sudden events in consumers' behavior and reflect it in the trust assessment. Adali et al. [2010] propose algorithmically quantifiable measures of trust based on communication behavior of members in a social network, with the premise that trust results in likely communication behaviors which are statistically different from random communications. Identifying such trust-like behaviors then enables the system to detect who trusts whom in the network.

User behaviors are an important aspect of trust in social networks. Current literature has focused on behaviors separately from the other aspects, namely attitudes and experiences. Future research needs to focus on a combination of all aspects for holistic analysis of trust in social networks.

7. SOCIAL TRUST EVALUATION MODELS

Approaches to trust computation can be roughly categorized as network-based trust models, interaction-based trust models, and hybrid trust models. The majority of the literature leverages on the social network structure.

7.1. Network Structure/Graph-Based Trust Models

Network structures affect the level of trust in social networks. High density in a network (i.e., higher interconnectedness between members) can yield a high level of trust [Buskens 1998]. Increases in both the in-degree and the out-degree in turn increase the level of trust a member can have in another member. The amount of information received is larger if a member receives information from members with a higher in-degree, therefore, receiving information from members with a higher in-degree increases the level of trust. Buskens [1998] draws some observations from his study of

social network structures: (i) members with a higher out-degree have higher levels of trust, (ii) levels of trust increase if members direct their ties more towards members with higher out-degrees, and (iii) while individual centralization (individual in the central location of the network) has a positive effect on the level of trust for the member involved, the average level of trust of all members decreases in the centralization of the whole network. Models that exploit the social network structure are typically based on the concepts of "Web of trust" or FOAF (Friend-Of-A-Friend). A trust network is usually created for each member. It represents the other members in the person's social network as nodes and the amount of trust he/she has for each of them as the edges. Various approaches are then used to traverse the network and determine trust between any two nodes. These approaches exploit the propagative nature of trust for trust evaluation. We review some of the major works.

Golbeck et al. [2003] propose a method for creating a trust network on the semantic Web by extending the FOAF schema to allow users to indicate a level of trust for people they know. The model specifies 9 levels of trust from "distrusts absolutely" to "trusts absolutely". Trust can be indicated on a general level or for specific areas (contexts). Users can specify multiple specific trust levels for the same entity/person for different contexts. The model uses an ontology to define different trust levels for the different contexts. The extended/trust-annotated FOAF graph is then used to infer trust values between nodes/people not directly connected to each other. Trust computation is done over the network structure using the weighted edges of the graph. In other work, Golbeck [2005b] proposes TidalTrust for deriving a trust relationship between two people in the social network using the FOAF vocabulary. The approach is based on the premise that neighbors with higher trust ratings are likely to agree with each other about the trustworthiness of a third party. Therefore, for a fixed trust rating, shorter paths have a lower average difference and higher trust ratings have a lower average difference. Zhang et al. [2006] expand Golbeck's trust model to include pairwise trust ratings and reliability factors of the entities in the network, using an edge-weighted graph to calculate trust. First, the similarity of two raters is calculated by comparing the ratings provided by them for the same provider. It is then employed to decide which neighbor's recommendation to follow. Comparing two recommendations, the recommendation from a rater that is more similar to the trustor will be chosen.

Ziegler and Lausen [2004] propose an approach, called Appleseed, to devise a local group trust matrix in the context of the semantic Web. The motivation for the approach is twofold: to use a partial trust graph exploration and to reduce computational complexity. The approach eliminates the need to explore a global trust graph in most cases, thus helping to reduce the computational complexity by limiting the scope of the computation to a reduced trust graph. Hang and Singh [2010] also employ a graph-based approach for measuring trust, with the aim to recommend a node in a social network using the trust network. The model uses the similarity between graphs to make recommendations. Zuo et al. [2009] propose an approach for computing trust in social networks using a set of trust chains and a trust graph. The model uses a trust certificate graph and calculates trust along a trust chain. In addition, it exploits the composability of trust in the form of fusion of relevant trust chains to form a base trust chain set.

Caverlee et al. [2008] propose a social trust model that exploits both social relationships and feedback to evaluate trust. Members provide feedback ratings after they have interacted with another member. The trust manager combines these feedback ratings to compute the social trust of the members. A member's feedback is weighted by their link quality (high link quality indicates more links with members having high trust ratings). Kuter et al. [2007] focus on the trust on information obtained from different social channels/chains. They propose a Bayesian trust inference model for

estimating the confidence on the trust information obtained from specific sources. In contrast to most "Web of trust" mechanisms that derive data from users' feedback, Kim [2008] explores building a Web of trust without using explicit user ratings. The model considers a user's reputation (expertise) and affinity for certain contexts/topics as main factors to derive trust connectivity and trust value. For example, user A is interested in reading science fiction novels and watching drama movies. User B writes reviews on movies. User C writes reviews on books. User A trusts user B in the context of movies and C in the context of books. The context can be derived from the user A, B, and C's activities in the online community. This means a trust value is derived based on the reputation of a provider such as B and C and the affinity of the user to different topics such as movie and book. This provides a much denser "Web of trust". The approach has three steps: (i) calculating users' expertise in a certain topic, which involves calculating the quality of reviews using the reputation of raters and then the reputation of writers, (ii) calculating the users' affinity to the category: the user affinity to the ratings is derived from the average number ratings and reviews provided by them in each category, and (iii) deriving degree of trust: the trust is derived from the user's affinity to the topic and another user's expertise on the topic.

Maheswaran et al. [2007] propose a gravity-based model for estimating trust. The trust model has two stages: first, the strengths of the friendships are recomputed along with the extent of the trusted social neighborhood for each user. This is based on the user's annotations of the connections s/he has with others with trust values or constraints. Second, the social neighborhood is used to compute the effective trust flow for users not in the social neighborhood. The model is based on the presumption that social relationships change over time and social relations may impose constraints on the trust relationships. The model also includes provenance of trust in social networks, where a user can ask questions about the trust value given by the underlying system.

Approaches that leverage network structures to compute trust capture one aspect of trust computation, namely, how members are related to each other and how trust flows through their network. They fail, however, to capture actual interactions between members. The volume, frequency, and even the nature of interaction are important indicators of trust in social networks. We now discuss trust models that take interactions as the basis for trust evaluation.

7.2. Interaction-Based Trust Models

In contrast to the models presented in the last section, some trust models in the literature only use interactions within the network to compute social trust. Liu et al. [2008] propose an approach for predicting trust in online communities using the interaction patterns/behaviors of the users. They identify two types of taxonomies representing user actions and possible interactions between pairs in the community: (i) user actions taxonomy for shared data such as reviews, posted comments, rating, etc., with metrics such as number/frequency of reviews, number/frequency of ratings, average length/number of comments given to reviews; and (ii) pair interactions taxonomy for different possible interactions/connections that could happen between two users, for example, connections between writers and raters, writers and writers, and raters and raters. The model also considers the time difference between two users' respective actions which form the connection, called the "temporal factor". They describe a supervised learning approach that automatically predicts trust between a pair of users using evidence derived from actions of individual users (user factors) as well as from interactions between pairs of users (interaction factors). These factors are then used to derive the corresponding features to train classifiers that predict trust between pairs of users.

Nepal et al. [2011] propose STrust, a social trust model based only on interactions within the social network. The model consists of two types of trust: the *popularity*

trust refers to the acceptance and approval of a member in the community, representing the trustworthiness of the member from the perspective of other members in the community; and the *engagement trust* refers to the involvement of the member in the community, representing the trust the member has towards the community. Popularity trust is derived from metrics such as how many members follow, read, and provide positive feedback on the member's posts. Engagement trust is derived from metrics such as how frequently the member visits the site/network, how many members s/he follows, and how many posts s/he reads and comments on. A combination of popularity trust and engagement trust forms the basis for determining the social trust in the community. The model aims to increase the social capital of the community by encouraging positive interactions within the community and, as a result, increase the social trust in the community.

Similarly, Adali et al. [2010] evaluate trust based on communication behavior of members in a social network. Behavioral trust is calculated based on two types of trust: conversation trust and propagation trust. Conversation trust specifies how long and/or how frequently two members communicate with each other. Longer and/or more frequent communication indicates more trust between the two parties. Similarly, propagation of information obtained from one member to other members in the network indicates high degree of trust placed on the information and implicitly on the member that created the information.

Interaction-based social trust models consider interactions in the community to compute trust, but ignore the social network structure. Social network structure provides important information about how members in a community relate to each other and is a significant source of information for social trust computation. Therefore, social trust models should consider both graph structures and interactions within the social networks to compute social trust. These models can be considered to be hybrid models. We discuss these models next.

7.3. Hybrid Trust Models

Hybrid trust models use both interactions and social network structure to compute social trust. Trifunovic et al. [2010] propose such a social trust model for opportunistic networks. Opportunistic networks enable users to participate in various social interactions with applications such as content distribution and microblogs. The model leverages the social network structure and its dynamics (conscious secure pairing and wireless contacts) and proposes two complementary approaches for social trust establishment: explicit social trust and implicit social trust. Explicit social trust is based on consciously established social ties. Each time two users interact, they exchange their friend lists and save them as friendship graphs. Trust is calculated on the friendship graph with a direct link/friend having the highest trust value of 1. As the number of links between two users grows, trust decreases proportionately. Implicit trust is based on frequency and duration of contact between two users. It uses two metrics: familiarity and similarity of the nodes. Familiarity describes the length of the interactions/contacts between the two nodes. Similarity describes the degree of coincidence of the two nodes' familiar circles. In this model, explicit social trust evaluation is based on network structure whereas implicit trust evaluation is based on user's interactions in the network. This work considers only the duration and frequency of interactions. However, the nature of interactions is an important indicator of trust between two members. If two members interact frequently but the interaction is negative, for example, they are having an argument, then this does not indicate trust between the members. In such cases also, this model would consider trust to be high. The literature on hybrid social trust models is limited. This presents an interesting area for further research.

8. TRUST DISSEMINATION MODELS

There could be many ways of disseminating trust information. Recommendation is one approach for trust value dissemination within a social network. Visualization is another approach. We discuss each in turn.

8.1. Trust-Based Recommendation Models

Trust-based recommendation usually involves constructing a trust network where nodes are users and edges represent the trust placed on them. The goal of a trust-based recommendation system is to generate personalized recommendations by aggregating the opinions of other users in the trust network. Recommendation techniques that analyze trust networks were found to provide very accurate and highly personalized results. Hang et al. [2010] use a graph-based approach to recommend a node in a social network using similarity in trust networks. Massa and Aversani [2007] propose a trust-based recommendation system where it is possible to search for trustable users by exploiting trust propagation over the trust network. Andersen et al. [2008] explore an axiomatic approach for trust-based recommendation and propose several recommendation models, some of which are incentive compatible (i.e., malicious members cannot entice other members to provide false/misleading trust information and trust links because it is always in the interest of the member to provide factual information).

Hess [2006, 2008] extends trust-based recommendations for single items such as movies to linked resources. For this purpose, she builds a second type of network, called a document reference network. Recommendations for documents are typically made by reference-based visibility measures which consider a document to be more important if it is often referenced by important documents. Document and trust networks, as well as networks such as organization networks, are integrated in a multilayer network. This architecture allows for combining classical visibility measures with trust-based recommendations, giving trust-enhanced visibility measures.

Trust-based recommendation techniques provide a way of disseminating trust information within a social network. However, the social network providers would prefer to have a bird's-eye view of trust in the social network at any point in time. Trust visualization provides this mechanism for trust dissemination at network level. We discuss these models in the next section.

8.2. Visualization Models

Visualization of trust connections as a graph is another means for disseminating trust information. Graphs show the strength of connection between two nodes, meaning the connection routes between two nodes: a higher number of connections means a closer relationship. Many social network visualization tools are available in the Internet, such as SocNetV[6] (Social Network Visualization), NetVis[7] (Network Visualization) and Graphviz[8] (Graph Visualization) among others.

Vigas and Donath [2004] propose an alternative approach for visualization of social networks representing the frequency of connections over time (referred to as PostHistory). The authors observe the connections of participants using their email TO and CC headers. The application has a calendar and a panel to display the contacts. For each point in time (day in calendar), the contacts panel shows the contacts that are most frequently in touch. In contrast to graph visualizations that demonstrate the strength of connection between members in a social network, this visualization depicts the frequency of connection between the members. In a similar way, trust connections along

[6]http://socnetv.sourceforge.net.
[7]http://www.netvis.org/index.php.
[8]http://www.graphviz.org/.

with the amount of trust between members can be visualized using graphs. O'Donovan et al. [2007] propose a model that extracts negative information from the feedback comments on eBay, computes personalized and feature-based trust, and presents this information graphically. The graph shows the trust value and the trust strength calculated based on the number of transactions/comments between two users. Guerriero et al. [2009] propose a trust-based visualization of cooperation context between members. Bimrah et al. [2008] propose a visualization language for trust-related requirements elicitation. The language aims to help in understanding how trust can be modeled and reasoned when developing information systems.

Trust visualization approaches are very useful for the social network providers to analyze and determine the level of trust in the community. It helps them identify the most and least trustworthy members. In addition, the providers can take preemptive action such as introducing new interesting and relevant material/information if the trust level in the community decreases below a certain threshold. Trust visualization allows the provider to control the social network to encourage positive behavior and discourage disruptive behavior.

9. ANALYSIS

Table I shows a comparative evaluation of existing trust literature based on the classification criteria defined in Section 1. Most trust models in computer science use the relational facet of trust with trust based (partially) on direct past interactions. Use of other sociological and psychological facets/aspects such as calculative, emotional, cognitive, institutional, and dispositional in the formation of trust models has been limited. Some of these facets of trust come into play when making trust decisions. In computer science, the focus is on computing trust values, and usually, the trust decision is based on a peer exceeding a certain trust threshold or having the highest trust value. Sociology and psychology have studied the effects of various aspects of trust such as calculative, relational, emotional, and cognitive on the trust decision-making process. These aspects of trust need to be considered in computer science trust decision making, and especially in social networks to reflect the human trust decision-making process. Similarly, very few models consider the context-specific nature of trust. Specifically, it is important to devise methods for inferring trust from one scope to another; also, it is debatable whether in fact it should be done. For example, a manufacturer releases a new product in the market. People's trust of the new product will be based on their trust of the existing products of the manufacturer as well as their trust of the manufacturer itself. In this case, it makes sense to infer trust from one context/scope to another. However, in the case of trusting a person as a doctor and trusting his/her as a mechanic, trust may not be transferable. How to identify cases where trust can or cannot be transferred from one context to another is an interesting question. This also raises a related issue of bootstrapping trust, that is, assigning initial trust value to a newcomer in the network. If trust can be inferred from another context, and such trust information is available about the newcomer, then trust inference can be used as a mechanism for bootstrapping. Malik and Bouguettaya [2009] propose various schemes for bootstrapping trust in the Web services domain. In a similar vein, trust bootstrapping needs to be thoroughly examined for the social networks domain.

Table I also shows that various properties of trust have received little attention in the literature, such as asymmetry, self-reinforcement, and event sensitivity. Similarly, the majority of trust evaluation models are based on network/graph structure. Graphs typically consider the volume and frequency of interactions, but neglect an important aspect of social networks, namely duration and intimacy of interactions, and the types of interactions. Since social networks are typically interaction intensive, different types of interactions provide a unique insight into trust formation within the network and

Table I. Comparison of Existing Trust Literature

Method	Origin Discipline	Trust Properties	Trust Computation Model	Trust Information Collection	Trust Evaluation	Trust Dissemination	Malicious Attack Resistance	Application Domains
EigenTrust-Kamvar *et al.*(2003)	C	Pr, Sj	LN	E	G	TR	Y	P2P
PeerTrust-Xiong *et al.* (2004)	C	Dy, Cs, Sj	LN	E	G	TR	Y	P2P
Yu *et al.* (2004)	C	Pr, Sj	LN	E	G	TR	Y	P2P
TidalTrust-Golbeck *et al.* (2005)	C	Pr, Sj	Prob.	E	G	TR	N	SN
Josang *et al.* (2006)	C	Dy, Pr, Sj	Prob.	BI	G	TR	N	P2P
Zhang *et al.* (2006)	S	Pr, Sj	LN	E	G	TR	N	SN
SUNNY-Kuter *et al.* (2007)	C	Sj	BN	B	G	_	N	SN
Maheswaran *et al.* (2007)	C	Pr, Cs, Sj	LN	E	G	TR	N	SN
PowerTrust-Zhou *et al.* (2007)	C	Pr, Sj	BN	E	N	_	Y	P2P, SN
Caverlee *et al.* (2008)	S	Dy	LN	B, E	G	TR	Y	P2P, SN
Liu *et al.* (2008)	C	Dy	Binary Classification	B	I	_	N	SN, e-commerce
Paradesi *et al.* (2008/2009)	C	Cp	BN	E	_	_	N	WS
Yan *et al.* (2009)	C	Sj	LN	B	_	_	N	MA
Zuo *et al.* (2009)	C	Pr, Cp	LN	TC	G	_	N	SN
Adali *et al.* (2010)	S	_	Log.	B	G	_	N	SN
Nepal *et al.* (2010)	S	Es	Prob.	B	_	_	N	WS, SN
Trifunovic *et al.* (2010)	S	Pr, Sj	LN	B, E	H	_	Y	SN
Nepal *et al.* (2011)	S	Sj, Dy, Cs	LN	B	I	_	N	SN

Origin Discipline	Trust Properties	Trust Computation Model	Trust Information Collection
P: Psychology, S: Sociology, C: Computer Science	Cs: Context-specific, Dy: Dynamic, Pr: Propagative, Cp: Composable, Sj: Subjective, Es: Event Sensitive	Log.: Logarithmic, Prob. : Probabilistic, BN: Bayesian Networks, LN: Linear Model (Sum or product)	B: Behaviour, E: Experience, BI: Belief, TC: Trust Certificate

Trust Evaluation	Trust Dissemination	Attack Resistance	Application Domains
G: Graph-based, I: Interaction-based, H: Hybrid, -: Not specified	TR: Trust-based Recommendation, VZ: Visualisation, -: Not specified	Y: Malicious attacks considered, N: Malicious attacks not considered	P2P: Peer-to-peer networks SN: Social Networks, WS: Web Services, MA: Mobile Applications

need to be considered together with the network structure. Additionally, the type and direction of interaction provides further information about the trust relationship. Typically, interactions could be active such as contributing posts, comments/feedbacks, sending friend requests, or passive such as reading others' posts and responding to friend requests. Similarly, the direction of interaction indicates whether the member usually initiates interaction with others or only responds to others' initiations. All of these factors could indicate different types of trust relationships and trust levels within the community. These aspects are significant in social networks and provide interesting avenues for further research.

As shown by Table I, trust information collection is typically based on user behavior or user experience. User attitudes also play a significant role in how a member interacts/behaves with other members in the community and can be a source of trust information. User attitude information is specially significant in analyzing interactions within a community. Another relevant aspect is tie strength between members of a social network, as characterized by the amount of time invested, the emotional intensity, and the intimacy between two members of a social network. In any social network, tie strengths between the members could fall anywhere in the spectrum from strong to

weak. Strong tie defines the circle of trusted people with whom a member has already established a trusted relationship, whereas weak ties are merely acquaintances. Intuitively, strong ties indicate the existence of trust in the relationship. However, weak ties are also important. Research [Granovetter 1973] has shown that weak ties are typically the source of new information in a member's network, but trust of the information may be low since it comes from a weak tie. Similarly, strong ties typically do not lead to new information, but any information originating from strong ties will be trusted more because of the strength of the tie. Tie strength adds a very interesting dimension to understanding trust. Deriving a trust model based on tie strength is an interesting area of future research.

Another area requiring further research in social networks trust is the visualization of trust. As can be seen in Table I, most current trust models use trust-based recommendation as the means for disseminating trust information. This is an effective technique for disseminating trust information within the community. However, the social network providers require a different kind of trust information dissemination. A visualization of trust in the community at a point in time gives a snapshot of the community trust level. Such a visualization could include different types of interactions within the community. This may help the social network provider identify whether there is a need to stimulate the community by providing relevant materials, or by introducing competitions, games, etc. This raises a related issue of sustainability of a social network. At what point, with what level of member engagement and participation can a social network community be considered sustainable? At what level of member participation should the provider intervene? Current literature has typically focused on trust aspects from members' point of view. There is a need to consider trust from the community provider's point of view.

Another significant aspect of a trust system is its ability to resist malicious attacks designed to subvert the system. Table I shows that most trust systems designed for P2P systems consider the possibility of malicious attacks. However, most trust systems designed for social networks have ignored the aspect of robustness against attacks. A survey by Josang et al. [2007] also highlights the importance of robustness in trust models. Similarly, recent research [Dwyer et al. 2007; Young and Quan-Haase 2009] has highlighted the lack of privacy in social networks. Privacy concerns prevent many members from freely interacting and contributing in the community, indicating a lack of trust of the service/network/platform and the platform provider. Since the main aim of social networks is to provide a forum for free and unhindered communication, privacy concerns create a major roadblock in achieving this goal. Any social network would therefore need to address the privacy concerns of the members to be unconditionally accepted by its members and ultimately to be successful.

Due to the similar network-based structure of P2P systems and social networks, it may appear as though a trust system developed for a P2P system could be directly implemented and used in social networks. However, these two types of networks differ significantly. In P2P systems, each peer is aiming to look after its own interests, and, typically, the trust system is distributed, that is, each peer computes its trust of other peers individually and shares them with its immediate neighbors. In social networks, the goal is to benefit the whole community with open sharing of information, opinions, and experiences. Therefore, as discussed earlier, various factors such as the type, duration, direction, and strength of interactions play a major role in determining trust in social networks. Typically, individual members would not be bothered about trust computation. Therefore, the social network would need to provide a centralized trust model considering the interactions in the community. Also, member-to-member trust is the focus of peer-to-peer systems, whereas in social networks, trust between the member and the social network service, and trust between the member and the social network

provider are equally important. All of these aspects need to be considered in selecting and developing a trust model in any social network application. Another significant issue in social networks trust management is identification of when a social network community becomes a trust community as defined in Section 1. At what levels of trust between members, trust between members and the service, and trust between members and the provider can the social network be considered a true trust community is a very interesting and challenging question.

10. CONCLUSIONS

We presented a comprehensive review of trust in social networks. We examined the definitions and measurements of trust through the prisms of sociology, psychology, and computer science. This study identified the various facets/aspects of trust as: calculative, relational, emotional, cognitive, institutional/system, and dispositional. The study also identified the various properties of trust: context dependent, dynamic, transitive, propagative, composable, personalized, asymmetric, self-reinforcing, and event sensitive. The self-reinforcing and event-sensitive aspects of trust have received relatively less attention in the literature. Although many aspects of trust have been studied in different disciplines, the study of trust in social networks is still in an early stage. Trust models in social networks can be largely regarded as adaptations of models from other disciplines to social networks. Therefore, trust models in social networks are yet to include most aspects of trust in trust modeling.

We next discussed social networks and their evolution from human to human networks to Web-based social networks. The discussion also covered the properties of social networks, and why trust is important. Understanding the human social networks and their properties provides an insight into Web-based social networks, and how trust can be computed using principles from sociology. The most significant aspect of a social network is its social capital, which refers to the collective value associated with the social network. Social capital can be harnessed to cultivate trust in social networks. We discussed the differences and similarities between social capital and social trust and described an approach to derive social trust from social capital. From this perspective, we identified that trust models for social networks should cover two aspects of trust: sociological and computational. The sociological aspect of trust includes emotion, behavior, attitude, and experience of the members. The computational aspect should provide a notion of capturing and computing these sociological values. We reviewed social trust literature from both of these perspectives. Although a number of solutions have been proposed in the literature, a holistic solution for building trust community in social networks is yet to be developed.

REFERENCES

Abdul-Rahman, A. and Hailes, S. 2000. Supporting trust in virtual communities. In *Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS'00).* IEEE Computer Society, 1–9.

Adali, S., Escriva, R., Goldberg, M. K., Hayvanovych, M., Magdon-Ismail, M., Szymanski, B. K., Wallace, W. A., and Williams, G. 2010. Measuring behavioral trust in social networks. In *Proceedings of the IEEE International Conference on Intelligence and Security Informatics (ISI'10).* 150–152.

Alesina, A. and La Ferrara, E. 2002. Who trusts others? *J. Public Econ. 85*, 1, 207–234.

Andersen, R., Borgs, C., Chayes, J., Feige, U., Flaxman, A., Kalai, A., Mirrokni, V., and Tennenholtz, M. 2008. Trust-based recommendation systems: An axiomatic approach. In *Proceeding of the 17th International Conference on World Wide Web (WWW'08).* ACM Press, New York, 199–208.

Artz, D. and Gil, Y. 2007. A survey of trust in computer science and the semantic web. *Web Semantics 5,* 2, 58–71.

Azer, M. A., El-Kassas, S. M., Hassan, A. W. F., and El-Soudani, M. S. 2008. A survey on trust and reputation schemes in ad hoc networks. In *Proceedings of the 3rd International Conference on Availability, Reliability and Security.* IEEE Computer Society, Los Alamitos, CA, 881–886.

BARNES, J. A. 1954. Class and committees in a norwegian island parish. *Hum. Relat. 7*, 1, 39–54.

BEATTY, P., REAY, I., DICK, S., AND MILLER, J. 2011. Consumer trust in e-commerce web sites: A metastudy. *ACM Comput. Surv. 43*, 3, 1–46.

BIMRAH, K. K., MOURATIDIS, H., AND PRESTON, D. 2008. Modelling trust requirements by means of a visualization language. In *Proceedings of the Conference on Requirements Engineering Visualization (REV'08)*. IEEE Computer Society, Los Alamitos, CA, 26–30.

BOLTZMANN, L. 1964. *Lectures on Gas Theory*. Translated by Stephen G. Brush. University of California Press, Berkeley.

BRUNIE, A. 2009. Meaningful distinctions within a concept: Relational, collective, and generalized social capital. *Social Sci. Res. 38*, 2, 251–265.

BUSKENS, V. 1998. The social structure of trust. *Social Netw. 20*, 3, 265–289.

CASTELFRANCHI, C., CONTE, R., AND PAOLUCCI, M. 1998. Normative reputation and the costs of compliance. *J. Artif. Soc. Social Simul. 1*, 3.

CAVERLEE, J., LIU, L., AND WEBB, S. 2008. Socialtrust: Tamper-resilient trust establishment in online communities. In *Proceedings of the 8th ACM/IEEE-CS Joint Conference on Digital Libraries (JCDL'08)*. ACM Press, New York, 104–114.

CHALLENER, D., YODER, K., CATHERMAN, R., SAFFORD, D., AND VAN DOORN, L. 2007. *A Practical Guide to Trusted Computing*. 1st Ed. IBM Press.

CHANG, E., DILLON, T. S., AND HUSSAIN, F. 2006. *Trust and Reputation for Service-Oriented Environments: Technologies for Building Business Intelligence and Consumer Confidence*. Wiley Periodicals.

CHEN, H.-C. AND CHEN, A. L. P. 2001. A music recommendation system based on music data grouping and user interests. In *Proceedings of the 10th International Conference on Information and Knowledge Management (CIKM'01)*. ACM Press, New York, 231–238.

CHEN, L. AND LI, J. 2010. Revocation of direct anonymous attestation. In *Proceedings of the 2nd International Conference on Trusted Systems (INTRUST'10)*. 128–147.

CHRISTIANSON, B. AND HARBISON, W. 1996. Why isn't trust transitive? In *Proceedings of the Security Protocols Workshop*. 171–176.

CLARIDGE, T. 2004. Social capital and natural resource management. M.S. thesis, Australia. http://www.socialcapitalresearch.com/literature/nrm.html.

COLEMAN, J. S. 1988. Social capital in the creation of human capital. *Amer. J. Sociology 94*, 1, 95–120.

COLEMAN, J. S. 1990. *Foundations of Social Theory*. Belknap Press, Cambridge, MA.

COOK, K. S., YAMAGISHI, T., CHESHIRE, C., COOPER, R., MATSUDA, M., AND MASHIMA, R. 2005. Trust building via risk taking: A cross-societal experiment. *Social Psychol. Quart. 2*, 68, 121–142.

COULTER, K. S. AND COULTER, R. A. 2002. Determinants of trust in a service provider: The moderating role of length of relationship. *J. Service. Market. 16*, 1, 35–50.

DOHMEN, T., FALK, A., HUFFMAN, D., AND SUNDE, U. 2006. The intergenerational transmission of risk and trust attitudes. IZA working paper. http://www.cens.uni-bonn.de/team/board/armin-falk/the-intergenerational-transmission-of-risk-and-trust-attitudes-review-of-economic-studies-2012-792-645-677-with-thomas-dohmen-david-huffman-and-uwe-sunde..pdf.

DUMOUCHEL, P. 2005. Trust as an action. *Euro. J. Sociol. 46*, 417–428.

DWYER, C., HILTZ, S. R., AND PASSERINI, K. 2007. Trust and privacy concern within social networking sites: A comparison of facebook and myspace. In *Proceedings of the 13th Americas Conference on Information Systems*.

ELSALAMOUNY, E., SASSONE, V., AND NIELSEN, M. 2010. HMM-based trust model. In *Proceedings of the 6th International Workshop on Formal Aspects on Security and Trust (FAST'09)*. Lecture Notes in Computer Science, vol. 5983, Springer, 21–35.

FUKUYAMA, F. 1995. *Trust: The Social Virtues and the Creation of Prosperity*. Free Press, New York.

GILBERT, E. AND KARAHALIOS, K. 2009. Predicting tie strength with social media. In *Proceedings of the 27th International Conference on Human Factors in Computing Systems (CHI'09)*. ACM Press, New York, NY, 211–220.

GOLBECK, J. 2005a. Personalizing applications through integration of inferred trust values in semantic web-based social networks. In *Proceedings of the Semantic Network Analysis Workshop at the 4th International Semantic Web Conference*.

GOLBECK, J. 2006a. Combining provenance with trust in social networks for semantic web content filtering. In *Proceedings of the International Conference on Provenance and Annotation of Data (IPAW'06)*. L. Moreau and I. Foster, Eds., Lecture Notes in Computer Science Series, vol. 4145, Springer, 101–108.

GOLBECK, J. 2006b. Trust on the world wide web: A survey. *Found. Trends Web Sci. 1*, 2, 131–197.

GOLBECK, J. 2007. The dynamics of web-based social networks: Membership, relationships, and change. *First Monday 12*, 11.

GOLBECK, J., PARSIA, B., AND HENDLER, J. 2003. Trust networks on the semantic web. In *Proceedings of the 7th International Workshop on Cooperative Intelligent Agents*. 238–249.

GOLBECK, J. A. 2005b. Computing and applying trust in web-based social networks. Ph.D. thesis, University of Maryland at College Park, MD.

GRANDISON, T. AND SLOMAN, M. 2000. A survey of trust in internet applications. *IEEE Comm. Surv. Tutorials 3*, 4.

GRANOVETTER, M. 1973. The strength of weak ties. *Amer. J. Sociology 78*, 1360–1380.

GRANOVETTER, M. 1985. Economic action and social structure: The problem of embeddedness. *Amer. J. Sociol. 91*, 481–510.

GROSS, R. AND ACQUISTI, A. 2005. Information revelation and privacy in online social networks. In *Proceedings of the ACM Workshop on Privacy in the Electronic Society (WPES'05)*. ACM Press, New York, 71–80.

GUERRIERO, A., KUBICKI, S., AND HALIN, G. 2009. Trust-oriented multi-visualization of cooperation context. In *Proceedings of the 2nd International Conference in Visualisation (VIZ'09)*. IEEE Computer Society, Los Alamitos, CA 96–101.

HANCHARD, S. 2008. Measuring trust and social networks - Where do we put our trust online? Hitwise. http://weblogs.hitwise.com/sandra-hanchard/2008/09/measuring_trust_ and_social_net.html.

HANG, W. C. AND SINGH, M. P. 2010. Trust based recommendation based on graph similarities. http://www.csc.ncsu.edu/faculty/mpsingh/papers/mas/aamas-trust-10-graph.pdf.

HAYTHORNTHWAITE, C. 2005. Social networks and internet connectivity effects. *Inf. Comm. Soc. 8*, 2, 125–147.

HELBING, D. 1994. A mathematical model for the behavior of individuals in a social field. *J. Math. Sociol. 19*, 3, 189–219.

HELBING, D. 1992. A mathematical model for attitude formation by pair interactions. *Behav. Sci. 37*, 3, 190–214.

HERLOCKER, J. L., KONSTAN, J. A., AND RIEDL, J. 2000. Explaining collaborative filtering recommendations . In *Proceedings of ACM Conference on Computer Supported Cooperative Work (CSCW'00)*. 241–250.

HESS, C. 2006. Trust-based recommendations for publications: A multi-layer network approach. *IEEE Tech. Commit. Digital Librar. Bull. 2*, 2.

HESS, C. 2008. Trust-based recommendations in multi-layer networks. Ph.D. thesis, Otto-Friedrich University Bamberg/University Paris-Sud.

HOFFMAN, K., ZAGE, D., AND NITA-ROTARU, C. 2009. A survey of attack and defense techniques for reputation systems. *ACM Comput. Surv. 42*, 1–31.

HOLMES, J. 1991. Trust and the appraisal process in close relationships. In *Advances in Personal Relationships*, W. Jones and D. Perlman, Eds., Jessica Kingsley, London, 57–104.

HUANG, F. 2007. Building social trust: A human-capital approach. *J. Institut. Theor. Econ. 163*, 4, 552–573.

HUGHES, D., COULSON, G., AND WALKERDINE, J. 2005. Free riding on gnutella revisited: The bell tolls? *IEEE Distrib. Syst. Online 6*, 6, 1.

HUMPHREYS, L. 2007. Mobile social networks and social practice: A case study of dodgeball. *J. Comput.-Mediated Comm. 13*, 1, 341–360.

HUYNH, T. D., JENNINGS, N. R., AND SHADBOLT, N. R. 2006. Certified reputation: How an agent can trust a stranger. In *Proceedings of the 5th International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS'06)*. New York, NY, 1217–1224.

JACKSON, P. J. 1999. *Virtual Working: Social and Organisational Dynamics.* Routledge, New York.

JAEGER, P. T., SHNEIDERMAN, B., FLEISCHMANN, K. R., PREECE, J., QU, Y., AND WU, P. F. 2007. Community response grids: E-government, social networks, and effective emergency management. *Telecomm. Policy 31*, 10–11, 592–604.

JAMIESON, K. AND CAPPELLA, J. 2009. *Echo Chamber: Rush Limbaugh and the Conservative Media Establishment.* Oxford University Press.

JOHNSON, D. AND GRAYSON, K. 2005. Cognitive and affective trust in service relationships. *J. Bus. Res. 58*, 4, 500–507.

JONES, K. 1996. Trust as an affective attitude. *Ethics 107*, 1, 4–25.

JOSANG, A. 2001. A logic for uncertain probabilities. *Int. J. Uncert., Fuzzin. Knowl.-Based Syst. 9*, 3, 279–311.

JOSANG, A. AND GOLBECK, J. 2009. Challenges for robust trust and reputation systems. In *Proceedings of the 5th International Workshop on Security and Trust Management (STM'09)*.

JOSANG, A., GRAY, E., AND KINATEDER, M. 2003. Analysing topologies of transitive trust. In *Proceedings of the 1st Workshop on Formal Aspects in Security and Trust (FAST'03)*. 9–22.

JOSANG, A., HAYWARD, R., AND POPE, S. 2006. Trust network analysis with subjective logic. In *Proceedings of the 29th Australasian Computer Science Conference (ACSC'06)*. Australian Computer Society, Hobart, Australia, 85–94.

JOSANG, A. AND ISMAIL, R. 2002. The beta reputation system. In *Proceedings of the 15th Bled Conference on Electronic Commerce*. 891–900.

JOSANG, A., ISMAIL, R., AND BOYD, C. 2007. A survey of trust and reputation systems for online service provision. *Decis. Support Syst. 43*, 2, 618–644.

JURCA, R. AND FALTINGS, B. 2003. An incentive compatible reputation mechanism. In *Proceedings of the IEEE Conference on E-Commerce (CEC'03)*. 396–409.

KAMVAR, S. D., SCHLOSSER, M. T., AND GARCIA-MOLINA, H. 2003. The eigentrust algorithm for reputation management in p2p networks. In *Proceedings of the 12th International Conference on World Wide Web (WWW'03)*. ACM Press, New York, 640–651.

KAUTZ, H., SELMAN, B., AND SHAH, M. 1997. Referral web: Combining social networks and collaborative filtering. *Comm. ACM 40*, 63–65.

KEITH, S. AND COULTER, R. A. C. 2002. Determinants of trust in a service provider: The moderating role of length of relationship. *J. Services Market. 16*, 1, 35–50.

KERR, R. AND COHEN, R. 2009. Smart cheaters do prosper: Defeating trust and reputation systems. In *Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems (AAMAS'09)*. Vol. 2, 993–1000.

KIM, Y. A. 2008. Building a web of trust without explicit trust ratings. In *Proceedings of the 24th IEEE International Conference on Data Engineering Workshop*. 531–536.

KLEINFELD, J. 2002. The small world problem. *Soc. Social Sci. Public Policy 39*, 61–66.

KLOS, T. B. AND LA POUTRE, H. 2005. Decentralized reputation-based trust for assessing agent reliability under aggregate feedback. In *Trusting Agents for Trusting Electronic Societies*, Springer, 10–128.

KOLLOCK, P. 1994. The emergence of exchange structures: An experimental study of uncertainty, commitment, and trust. *Amer. J. Sociol. 100*, 2, 313–345.

KOMIAK, S. X. AND BENBASAT, I. 2004. Understanding customer trust in agent-mediated electronic commerce, web-mediated electronic commerce, and traditional commerce. *Inf. Technol. Manag. 5*, 181–207.

KUAN, H. AND BOCK, G. 2005. The collective reality of trust: An investigation of social relations and networks on trust in multi-channel retailers. In *Proceedings of the 13th European Conference on Information Systems (ECIS'05)*.

KUTER, U. AND GOLBECK, J. 2007. Sunny: A new algorithm for trust inference in social networks using probabilistic confidence models. In *Proceedings of the 22nd National Conference on Artificial Intelligence*. AAAI Press, 1377–1382.

LAWLER, E. J. AND YOON, J. 1996. Commitment in exchange relations: Test of a theory of relational cohesion. *Amer. Sociol. Rev. 61*, 89–108.

LAZARSFELD, P. AND MERTON, R. 1954. Friendship as a social process: A substantive and methodological analysis. In *Freedom and Control in Modern Society*, M. Berger, T. Abel, and C. H. Page, Eds., Van Nostrand, New York, 18–66.

LEVIN, D. Z., CROSS, R., AND ABRAMS, L. C. 2004. The strength of weak ties you can trust: The mediating role of trust in effective knowledge transfer. *Manag. Sci. 50,* 1477–1490.

LEWIS, J. D. AND WEIGERT, A. 1985. Trust as a social reality. *Social Forces 63*, 4, 967–985.

LIKERT, R. 1932. A technique for the measurement of attitudes. *Archiv. Psychol. 140*, 1, 1–55.

LIU, H., LIM, E.-P., LAUW, H. W., LE, M.-T., SUN, A., SRIVASTAVA, J., AND KIM, Y. A. 2008. Predicting trusts among users of online communities: An epinions case study. In *Proceedings of the 9th ACM Conference on Electronic Commerce (EC'08)*. ACM Press, New York, 310–319.

MAHESWARAN, M., TANG, H. C., AND GHUNAIM, A. 2007. Towards a gravity-based trust model for social networking systems. In *Proceedings of the International Conference on Distributed Computing Systems Workshops*. IEEE Computer Society, Los Alamitos, CA, 24.

MALIK, Z., AKBAR, I., AND BOUGUETTAYA, A. 2009. Web services reputation assessment using a hidden markov model. In *Proceedings of the 7th International Joint Conference on Service-Oriented Computing (ICSOC-ServiceWave'09)*. 576–591.

MALIK, Z. AND BOUGUETTAYA, A. 2009. Reputation bootstrapping for trust establishment among web services. *IEEE Internet Comput. 13*, 40–47.

MANIKRAO, U. S. AND PRABHAKAR, T. V. 2005. Dynamic selection of web services with recommendation system. In *Proceedings of the International Conference on Next Generation Web Services Practices (NWESP'05)*. IEEE Computer Society, Los Alamitos, CA, 117–121.

MARMOL, F. G. AND PEREZ, G. M. 2011. Trust and reputation models comparison. *Internet Res. 21*, 138–153.

MARSH, S. P. 1994. Formalising trust as a computational concept. Ph.D. thesis, University of Stirling.

MASSA, P. AND AVESANI, P. 2007. Trust-aware recommender systems. In *Proceedings of the 1st ACM Conference on Recommender Systems (RecSys'07)*. ACM Press, New York.

MCLEOD, A. AND PIPPIN, S. 2009. Security and privacy trust in e-government: Understanding system and relationship trust antecedents. In *Proceedings of the 42nd Hawaii International Conference on System Sciences (HICSS'09)*. 1–10.

MCPHERSON, M., LOVIN, L. S., AND COOK, J. M. 2001. Birds of a feather: Homophily in social networks. *Ann. Rev. Sociol. 27*, 1, 415–444.

MIKA, P. 2007. *Social Networks and the Semantic Web*. Springer.

MILES, R. E. AND CREED, W. E. D. 1995. Organizational forms and managerial philosophies: A descriptive and analytical review. *Res. Organizat. Behav. 17*, 333–372.

MILGRAM, S. 1967. The small world problem. *Psychol. Today 1*, 1, 60–67.

MOIBUS, M. AND QUOC-ANH, D. 2004. Social capital in social networks. http://www.earthinstitute.columbia.edu/cgsd/documents/rosenblat.pdf.

MOLLERING, G. 2002. The nature of trust: From geog simmel to a theory of expectation, interpretation and suspension. *Sociol. 35*, 403–420.

MOLM, L. D., TAKAHASHI, N., AND PETERSON, G. 2000. Risk and trust in social exchange: An experimental test of a classical proposition. *Amer. J. Sociol. 5*, 105, 1396–1427.

MOMANI, M. AND CHALLA, S. 2010. Survey of trust models in different network domains. *Int. J. Ad Hoc Sensor Ubiq. Comput. 1*, 3, 1–19.

MORELAND, D., NEPAL, S., HWANG, H., AND ZIC, J. 2010. A snapshot of trusted personal devices applicable to transaction processing. *Personal Ubiq. Comput. 14*, 4, 347–361.

MUI, L. 2003. Computational models of trust and reputation: Agents, evolutionary games, and social networks. Ph.D. thesis. http://groups.csail.mit.edu/medg/people/lmui/docs/phddissertation.pdf.

MUI, L., MOHTASHEMI, M., AND HALBERSTADT, A. 2002. A computational model of trust and reputation. In *Proceedings of the 35th Hawaii International Conference on System Sciences (HICSS'02)*. IEEE Computer Society, Los Alamitos, CA, 188–196.

NAHAPIET, J. AND GHOSHAL, S. 1998. Social capital, intellectual capital, and the organizational advantage. *Academy Manag. Rev. 23*, 2, 242–266.

NEPAL, S., SHERCHAN, W., AND BOUGUETTAYA, A. 2010a. A behavior based trust model for service web. In *Proceedings of the IEEE International Conference on Service-Oriented Computing and Applications (SOCA'10)*. IEEE Computer Society, 1–4.

NEPAL, S., SHERCHAN, W., AND PARIS, C. 2011. STrust: A trust model for social networks. In *Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'11)*. 841–846.

NEPAL, S., ZIC, J., LIU, D., AND JANG, J. 2010b. Trusted computing platform in your pocket. In *Proceedings of the IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC'10)*. IEEE Computer Society, Los Alamitos, CA, 812–817.

O'DONOVAN, J., SMYTH, B., EVRIM, V., AND MCLEOD, D. 2007. Extracting and visualizing trust relationships from online auction feedback comments. In *Proceedings of the 20th International Joint Conference on Artificial Intelligence*. Morgan Kaufmann Publishers, San Francisco, 2826–2831.

PALDAM, M. 2000. Social capital: One or many? Definition and measurement. *J. Econ. Surv. 5*, 1, 629–653.

PARADESI, S., DOSHI, P., AND SWAIKA, S. 2009. Integrating behavioral trust in web service compositions. In *Proceedings of the IEEE International Conference on Web Services (ICWS'09)*. 453–460.

PUTNAM, R. 2000. *Bowling Alone: The Collapse and Revival of American Community*. Simon and Schuster, New York.

PUTNAM, R. D. 1995. Bowling alone: America's declining social capital. *J. Democracy 6*, 1, 65–78.

RESNICK, P., ZECKHAUSER, R., FRIEDMAN, E., AND KUWABARA, K. 2000. Reputation systems. *Comm. ACM 43*, 12, 45–48.

RICHARDSON, M., AGRAWAL, R., AND DOMINGOS, P. 2003. Trust management for the semantic web. In *Proceedings of the 2nd International Semantic Web Conference*. 351–368.

ROMER, P. M. 2000. Thinking and feeling. *Amer. Econ. Rev. 90*, 2, 439–443.

ROTTER, J. B. 1967. A new scale for the measurement of interpersonal trust. *J. Personality 35*, 4, 651–665.

ROTTER, J. B. 1971. Generalized expectancies for interpersonal trust. *Amer. Psychol. 26*, 1, 443–452.

ROUSSEAU, D. M., SITKIN, S. B., BURT, R. S., AND CAMERER, C. 1998. Not so different after all: A cross-discipline view of trust. *Academy Manag. Rev. 23*, 3, 393–404.

RUOHOMAA, S. AND KUTVONEN, L. 2005. Trust management survey. In *Proceedings of the 3rd International Conference on Trust Management (iTrust'05)*. Springer, 77–92.

RUOHOMAA, S., KUTVONEN, L., AND KOUTROULI, E. 2007. Reputation management survey. In *Proceedings of the 2nd International Conference on Availability, Reliability and Security (ARES'07)*. IEEE Computer Society, 103–111.

SABATER, J. 2002. Trust and reputation for agent societies. Ph.D. thesis, Autonomous University Of Barcelona, Spain. http://www.tesisenxarxa.net/TESIS_UAB/AVAILABLE/TDX-0123104172828//jsm1de1.pdf.

SABATER, J. AND SIERRA, C. 2002. Reputation and social network analysis in multi-agent systems. In *Proceedings of the 1st International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS'02)*. ACM Press, New York, 475–482.

SABATER, J. AND SIERRA, C. 2005. Review on computational trust and reputation models. *Artif. Intell. Rev. 24*, 33–60.

SCHILLO, M., FUNK, P., AND ROVATSOS, M. 2000. Using trust for detecting deceitful agents in artificial societies. *Appl. Artif. Intell. 14*, 8, 825–848.

SCHNEIDER, O. 2009. Trust-aware social networking: A distributed storage system based on social trust and geographic proximity. M.S. thesis. http://www.peerson.net/papers/oliver_da.pdf.

SCULLY, M. AND PREUSS, G. 1996. Two faces of trust: The roles of calculative and relational trust in work transformation. Tech. rep. working paper no. 3923–96, Massachusetts Institute of Technology.

SESHADRI, A., PERRIG, A., VAN DOORN, L., AND KHOSLA, P. K. 2004. SWATT: Software-based attestation for embedded devices. In *Proceedings of the IEEE Symposium on Security and Privacy*. 272–282.

SINGH, M. P., YU, B., AND VENKATRAMAN, M. 2001. Community-based service location. *Comm. ACM 44*, 49–54.

SINGH, S. AND BAWA, S. 2007. Privacy, trust and policy based authorization framework for services in distributed environments. *Int. J. Comput. Sci. 2*, 2, 85–92.

SONG, S., HWANG, K., ZHOU, R., AND KWOK, Y.-K. 2005. Trusted p2p transactions with fuzzy reputation aggregation. *IEEE Internet Comput. 9*, 6, 24–34.

SONG, W., PHOHA, V. V., AND XU, X. 2004. The hmm-based model for evaluating recommender's reputation. In *Proceedings of the IEEE International Conference on E-Commerce Technology for Dynamic E-Business*. IEEE, 209–215.

STAAB, S., BHARGAVA, B., LILIEN, L., ROSENTHAL, A., WINSLETT, M., SLOMAN, M., DILLON, T. S., CHANG, E., HUSSAIN, F. K., NEJDL, W., OLMEDILLA, D., AND KASHYAP, V. 2004. The pudding of trust: Managing the dynamic nature of trust. *IEEE Intell. Syst. 19*, 5, 74–88.

STURGIS, P., READ, S., HATEMI, P., ZHU, G., TRULL, T., WRIGHT, M., AND MARTIN, N. 2010. A genetic basis for social trust? *Polit. Behav. 32*, 2, 205–230.

SUH, B. AND HAN, I. 2002. Effect of trust on customer acceptance of Internet banking. *Electron. Commerce Res. Appl. 1*, 3–4, 247–263.

SURYANARAYANA, G., T. R. 2004. A survey of trust management and resource discovery technologies in peer-to-peer applications. Tech. rep. UCI-ISR-04-6, Institute for Software Research, University of California, Irvine.

SZTOMPKA, P. 1999. *Trust: A Sociological Theory.* Cambridge University Press.

TAYLOR, R. 2000. Marketing strategies: Gaining a competitive advantage through the use of emotion. *Competitiv. Rev. 10*, 146–152.

TOIVONEN, S., LENZINI, G., AND UUSITALO, I. 2006. Context-aware trust evaluation functions for dynamic reconfigurable systems. In *Proceedings of the Workshop on Models of Trust for the Web (MTW'06), held in Conjunction with the 15th International World Wide Web Conference*, T. Finin, L. Kagal, and D. Olmedilla, Eds., CEUR Workshop Proceedings Series, vol. 190.

TRIFUNOVIC, S., LEGENDRE, F., AND ANASTASIADES, C. 2010. Social trust in opportunistic networks. In *Proceedings of the INFOCOM IEEE Conference on Computer Communications Workshops*. IEEE, 1–6.

TYLER, T. R. 1990. *Why People Obey the Law.* Yale University Press, New Haven, CT.

TYLER, T. R. AND DEGOEY, P. 1996. Trust in organizational authorities: The influence of motive attributions on willingness to accept decisions. In *Trust in Organizations: Frontiers of Theory and Research*, R. M. Kramer and T. R. Tyler, Eds., Sage Publications, Thousand Oaks, CA.

VIGAS, F. B. AND DONATH, J. 2004. Social network visualization: Can we go beyond the graph? In *Proceedings of the Workshop on Social Networks for Design and Analysis: Using Network Information in CSCW*. 6–10.

VON LASZEWSKI, G., ALUNKAL, B., AND VELJKOVIC, I. 2005. Towards reputable grids: Scalable computing. *Pract. Exper. 6*, 3, 95–106.

WALDMAN, M., RUBIN, A. D., AND CRANOR, L. F. 2000. Publius: A robust, tamper-evident, censorship resistent web publishing system. In *Proceedings of the 9th USENIX Security Symposium*.

WALTER, F. E., BATTISTON, S., AND SCHWEITZER, F. 2009. Personalised and dynamic trust in social networks. In *Proceedings of the 3rd ACM Conference on Recommender Systems (RecSys'09)*. ACM Press, New York, 197–204.

WANG, T. AND LU, Y. 2010. Determinants of trust in e-government. In *Proceedings of the International Conference on Computational Intelligence and Software Engineering (CiSE'10)*. 1–4.

WANG, Y., HORI, Y., AND SAKURAI, K. 2007. Economic-inspired truthful reputation feedback mechanism in p2p networks. In *Proceedings of the 11th IEEE International Workshop on Future Trends of Distributed Computing Systems*. 80–88.

WANG, Y. AND VASSILEVA, J. 2007. A review on trust and reputation for web service selection. In *Proceedings of the 27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07)*. IEEE Computer Society, 25–32.

WATTS, D. J. 2003. *Six Degrees: The Science of a Connected Age*. W.W. Norton and Company, New York.

WEI-HANG, C. AND SINGH, M. P. 2010. Trust-based recommendation based on graph similarity. In *Proceedings of the 13th AAMAS Workshop on Trust in Agent Societies*. http://www.csc.ncsu.edu/faculty/mpsingh/papers/mas/aamas-trust-10-graph.pdf.

WELLMAN, B. 1996. For a social network analysis of computer networks: A sociological perspective on collaborative work and virtual community. In *Proceedings of the ACM SIGCPR/SIGMIS Conference on Computer Personnel Research (SIGCPR'96)*. ACM Press, New York, 1–11.

WELLMAN, B. 2004. The global village: Internet and community. *Arts Sci. Rev. 1*, 1, 26–30.

WILLIAMSON, O. E. 1993. Calculativeness, trust and economic organization. *J. Law Econ. 30*, 1, 131–145.

WISHART, R., ROBINSON, R., INDULSKA, J., AND JOSANG, A. 2005. Superstringrep: Reputation-enhanced service discovery. In *Proceedings of the 28th Australasian Conference on Computer Science (ACSC'05)*. Australian Computer Society, Darlinghurst, Australia, 49–57.

XIANG, R., NEVILLE, J., AND ROGATI, M. 2010. Modeling relationship strength in online social networks. In *Proceedings of the 19th International Conference on World Wide Web (WWW'10)*. ACM Press, New York, 981–990.

XIONG, L. AND LIU, L. 2003. A reputation-based trust model for peer-to-peer ecommerce communities. In *Proceedings of the 4th ACM Conference on Electronic Commerce (EC'03)*. ACM Press, New York, 228–229.

XIONG, L. AND LIU, L. 2004. PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities . *IEEE Trans. Knowl. Data Engin. 16,* 7, 843–857.

YAN, Z., NIEMI, V., DONG, Y., AND YU, G. 2008. A user behavior based trust model for mobile applications. In *Proceedings of the 5th International Conference on Autonomic and Trusted Computing*. 455–469.

YAN, Z. AND YAN, R. 2009. Formalizing trust based on usage behaviours for mobile applications. In *Proceedings of the 6th International Conference on Autonomic and Trusted Computing*. 194–208.

YANG, J., HU, X., AND ZHANG, H. 2007. Effects of a reputation feedback system on an online consumer-to-consumer auction market. *Decis. Support Syst. 44*, 1, 93–105.

YANIV, I. AND KLEINBERGER, E. 2000. Advice taking in decision making: Egocentric discounting and reputation formation. *Organiz. Behav. Hum. Decision Process. 83*, 2, 260–281.

YAO, J., CHEN, S., NEPAL, S., LEVY, D., AND ZIC, J. 2010. Truststore: Making amazon s3 trustworthy with services composition. In *Proceedings of the 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing (CCGRID'10)*. IEEE Computer Society, Los Alamitos, CA, 600–605.

YOUNG, A. L. AND QUAN-HAASE, A. 2009. Information revelation and internet privacy concerns on social network sites: A case study of facebook. In *Proceedings of the International Conference on Communities and Technologies*. 265–274.

YU, B. AND SINGH, M. P. 2000. A social mechanism for reputation management in electronic communities. In *Proceedings of the 4th International Workshop on Cooperative Information Agents (CIA'00)*. Springer, 154–165.

YU, B. AND SINGH, M. P. 2002. An evidential model of distributed reputation management. In *Proceedings of the 1st International Joint Conference on Autonomous Agents and Multi-Agent Systems (AAMAS'02)*. ACM Press, New York, 294–301.

YU, B., SINGH, M. P., AND SYCARA, K. 2004. Developing trust in large-scale peer-to-peer systems. In *Proceedings of the 1st IEEE Symposium on Multi-Agent Security and Survivability*. IEEE Computer Society, 1–10.

ZACHARIA, G. AND MAES, P. 2000. Trust management through reputation mechanisms. *Appl. Artif. Intell. 14*, 9, 881–907.

ZAJONC, R. 1980. Feeling and thinking: Preferences need no inferences. *Amer. Psychol. 35*, 2, 151–175.

ZAPPEN, J. P., HARRISON, T. M., AND WATSON, D. 2008. A new paradigm for designing e-government: Web 2.0 and experience design. In *Proceedings of the International Conference on Digital Government Research*. Digital Government Society of North America, 17–26.

ZARGHAMI, A., FAZELI, S., DOKOOHAKI, N., AND MATSKIN, M. 2009. Social trust-aware recommendation system: A t-index approach. In *Proceedings of the IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT'09)*. IEEE Computer Society, Los Alamitos, CA, 85–90.

ZHANG, Y., CHEN, H., AND WU, Z. 2006. A social network-based trust model for the semantic web. In *Proceedings of the 6th International Conference on Autonomic and Trusted Computing*. 183–192.

ZHANG, Y. AND FANG, Y. 2007. A fine-grained reputation system for reliable service selection in peer-to-peer networks. *IEEE Trans. Parallel Distrib. Syst. 18*, 8, 1134–1145.

ZHOU, R. AND HWANG, K. 2007. PowerTrust: A robust and scalable reputation system for trusted peer-to-peer computing. *IEEE Trans. Parallel Distrib. Syst. 18*, 4, 460–473.

ZIEGLER, C.-N. AND LAUSEN, G. 2004. Spreading activation models for trust propagation. In *Proceedings of the IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE'04)*. IEEE Computer Society, Los Alamitos, CA, 83–97.

ZUO, Y., HU, W.-C., AND O'KEEFE, T. 2009. Trust computing for social networking. In *Proceedings of the 6th International Conference on Information Technology: New Generations*. IEEE Computer Society, Los Alamitos, CA, 1534–1539.

Received September 2011; revised March 2012; accepted August 2012