[**Publication 1**] Zheng Yan and Silke Holtmanns, "Trust Modeling and Management: from Social Trust to Digital Trust", book chapter of *Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions*, IGI Global, 2007.

Trust Modeling and Management: from Social Trust to Digital Trust

Zheng Yan
Nokia Research Center
Itämerenkatu 11-13, 00180, Helsinki, Finland
Tele: +358 7180 36664
Fax: +358 7180 36214
Email: zheng.z.yan@nokia.com

Silke Holtmanns
Nokia Research Center
Itämerenkatu 11-13, 00180, Helsinki, Finland
Tele: +358 7180 41555
Fax: +358 7180 36214
Email: silke.holtmanns@nokia.com

Trust Modeling and Management: from Social Trust to Digital Trust

ABSTRACT

This chapter introduces trust modeling and trust management as a means of managing trust in digital systems. Transforming from a social concept of trust to a digital concept, trust modeling and management help in designing and implementing a trustworthy digital system, especially in emerging distributed systems. Furthermore, the authors hope that understanding the current challenges, solutions and their limitations of trust modeling and management will not only inform researchers of a better design for establishing a trustworthy system, but also assist in the understanding of the intricate concept of trust in a digital environment.

KEYWORDS

Trust, Trust Model, Trust Modeling, Trust Management, Trustworthy Digital System, Trust Evaluation, Security, Privacy, Trusted Computing, Distributed System, Electronic Commerce, Distributed System, Peer-to-peer System, Ad-Hoc Network, Grid Computing, Human-Machine Interaction, Software Engineering

Trust is beyond security. It is a solution for enhanced security.

INTRODUCTION

Trust plays a crucial role in our social life. Our social life is characterized by the trust relationships that we have. Trust between people can be seen as a key component to facilitate coordination and cooperation for mutual benefit. Social trust is the product of past experiences and perceived trustworthiness. We constantly modify and upgrade our trust in other people based on our feelings in response to changing circumstances. Often, trust is created and supported by a legal framework, especially in business environments or when financial issues are involved. The framework ensures that misbehavior can be punished with legal actions and increases the incentive to initiate a trust relationship. The legal framework decreases the risk of misbehavior and secures the financial transactions. With the rapid growth of global digital computing and networking technologies, trust becomes an important aspect in the design and analysis of secure distributed systems and electronic commerce. However, the existing legal frameworks are often focused on local legislation and are hard to enforce on a global level. The most popular examples are email spam, software piracy and a breach of warranty. Particularly, because legal regulation and control cannot keep pace with the development of electronic commerce, the extant laws in conventional commerce might not be strictly enforceable in electronic commerce. In addition, resorting to legal enforcement in electronic commerce might be impracticably expensive or even impossible, such as in the case of micro payment transactions (Ba, Whinston and Zhang 1999). This raises the importance of trust between interacting digital entities. People can not assume that the legal framework is able to provide the needed trustworthiness for their digital relationships, e.g. for an electronic transaction purpose. It has been a critical part of the process by which trust relationships are required to develop in a digital system. In particular, for some emerging technologies, such as MANET (Mobile Ad Hoc Networks), P2P (Peer-to-Peer) computing, and GRID virtual systems, trust management has been proposed as a useful solution to break through new challenges of security and privacy caused by the special characteristics of

these systems, such as dynamic topology and mobility (Yan, Zhang and Virtanen 2003; Yan 2006; Lin et al. 2004).

Trust is a very complicated phenomena attached to multiple disciplines and influenced by many measurable and non-measurable factors. It is defined in various ways for different purposes and cultures, even though in information technology area. Thereby, it is difficult to have a common definition for this comprehensive concept.

Establishing a trust relationship in digital networking environment involves more aspects than in the social world. This is because communications in the computing network rely on not only relevant human beings and their relationships, but also digital components. On the other hand, the visual trust impression is missing and need somehow to be compensated. Moreover, it is more difficult to accumulate accurate information for trust purposes in remote digital communications where information can be easily distorted or faked identities can be created. The mapping of our social understanding of trust into the digital world and the creation of trust models that are feasible in practice are challenging. Trust is a special issue beyond and will enhance a system security and personal privacy. Understanding the trust relationship between two digital entities could help selecting and applying feasible measures to overcome potential security and privacy risk. From social trust to digital trust, how can trust theory help in designing and implementing a trustworthy digital system? The literature suggests the usage of trust modeling and management. This book chapter aims to help readers understanding trust modeling and management in the emerging technologies. The reader is guided from the creation of a digital trust concept to the deployment of trust models for trust management in a digital environment.

BACKGROUND

The problem to create trust in the digital environment has led to a number of approaches, for example, expressing and modeling trust in a digital way, evaluating trust in a reputation system, rating agencies, certificate authorities that equip trading partners with certificates as trusted providers and brokers, trustworthy user interface design, etc. Current academic and industrial work related to trust covers a wide area of interest ranging from such aspects as perception of trust, cryptographic-security enforced trust solutions, trust modeling and management to trusted computing activities.

Perception of Trust Concept (from Social Trust towards Digital Trust)

What is trust and how is trust influenced? We will now examine the most common definitions of trust and start from a classical social trust concept that is supported by a legal framework to a concept for digital processing. Through the study of various definitions of trust, we explain the properties of trust relationships and classify the factors that influence trust.

Definitions of trust. The concept of trust has been studied in disciplines ranging from economics to psychology, from sociology to medicine, and to information science. It is hard to say what trust exactly is because it is a multidimensional, multidiscipline and multifaceted concept. We can find various definitions of trust in the literature. For example, it can be loosely defined as a state involving confident positive expectations about another's motives with respect to oneself in situations entailing risk (Boon and Holmes, 1991). This definition highlights three main characteristics of trust. First, a trust relationship involves at least two entities: a trustor and a trustee, reliant on each other for mutual benefit. Second, trust involves uncertainty and risk. There is no perfect guarantee to ensure that the trustee will live up to the trustor's expectation.

Third, the trustor has faith in the trustee's honesty and benevolence, and believes that the trustee will not betray his/her risk-assuming behavior.

Gambetta (1990) defined trust as trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent will perform a particular action, both before [we] can monitor such action (or independently of his capacity of ever to be able to monitor it) and in a context in which it affects [our] own action. Mayer, Davis, and Schoorman (1995) provided the definition of trust as the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party. These definitions point out another important main characteristic of trust: Trust is subjective. The level of trust considered sufficient is different for each individual in a certain situation. Trust may be affected by those actions that we cannot (digitally) monitor. The level of trust depends on how our own actions are in turn affected by the trustee's actions. Grandison and Sloman (2000) hold an opinion that trust is a qualified belief by a trustor with respect to the competence, honesty, security and dependability of a trustee within a special context.

McKnight and Chervany (2000, 2003) conducted analysis on the trust definitions and noted that trust is a concept hard to define because it is itself a vague term. Looking up the term "trust" in a dictionary may reveal many explanations since it is a cross-disciplinary concept. For example, from the sociologists' point of view, it is related to social structure. From the psychologists' point of view, it concerns personal trait. From the economists' point of view, it is a mechanism of economic choice and risk management. The definitions of trust can be classified based on the consideration of structural, disposition, attitude, feeling, expectancy, belief, intention, and behavior. There are suggestions to evaluate trust with regard to competence, benevolence, integrity, and predictability. But generally, these attributes are only applicable to very narrow scenarios and hard to measure.

Other expressions of trust are targeting at different context and technology areas, for example:

- ***On-line System:*** On-line trust is an attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited (Corritore, Kracher, and Wiedenbeck, 2003).
- ***Multi Agent System:*** In a multi-agent system, trust is a subjective expectation an agent has about another agent's future behavior (Mui, 2003).
- ***Software Engineering:*** From a software engineering point of view, trust is accepted dependability (Avizienis, Laprie, Randell, and Landwehr, 2004).
- ***Ad-Hoc Networks:*** For an ad hoc network, trust could be defined as the reliability, timeliness, and integrity of message delivery to a node's intended next-hop (Liu, Joy, and Thompson, 2004).

Denning (1993) emphasizes the importance of assessment for trust in a system, which is of particular importance in the digital environment, where the entities often just have digital artifacts to base their trust judgment on. The current paradigm for trusted computing systems holds that trust is a property of a system. It is a property that can be formally modeled, specified, and verified. It can be "designed into" a system using a rigorous design methodology. Trust is an assessment that a person, organization, or object can be counted on to perform according to a given set of standards in some domain of action. In particular, a system is trusted if and only if its users trust it. Trust itself is an assessment made by users based on how well the observed behavior of the system meets their own standards.

Common to many definitions are the notions of confidence, belief, faith, hope, expectation, dependence, and reliance on the goodness, strength, reliability, integrity, ability, or character of a person or entity. Generally, a trust relationship involves two entities: a trustor and a trustee. The trustor is the person or entity who holds confidence, belief, faith, hope, expectation, dependence, and reliance on the goodness, strength, reliability, integrity, ability, or character of another person or entity, which is the object of trust - the trustee.

Although the richness of the concept, we can still summarize the subjective and objective factors that are relevant to a decision of trust, as shown in Table 1.

Table 1: Factors influencing trust extracted from some definitions of trust

Factors related to trustee's objective properties	competence; ability; security; dependability; integrity; predictability; reliability; timeliness; (observed) behavior; strength
Factors related to trustee's subjective properties	Honesty; benevolence; goodness
Factors related to trustor's objective properties	assessment; a given set of standards; trustor's standards
Factors related to trustor's subjective properties	confidence; (subjective) expectations or expectancy; subjective probability; willingness; belief; disposition; attitude; feeling; intention; faith; hope; trustor's dependence and reliance
Context	situations entailing risk; structural; risk; domain of action

Factors influencing trust. Trust is subjective because the level of trust considered sufficient is different for each entity. It is the subjective expectation of the trustor on the trustee related to the trustee's behaviors that could influence the trustor's belief in the truestee. Trust is also dynamic as it is affected by many factors that are difficult to measure and monitor. It can be further developed and evolved due to good experiences about the trustee. Or it is sensitive to be decayed caused by one or several bad experiences. From the digital system point of view, trust is a kind of assessment on the trustee based on a number of referents, e.g. competence, security, reliability, etc. Trust is influenced by a number of factors. Those factors can be classified into five categories, as shown in Figure 1.

From the digital system point of view, we pay more attention to the objective properties of both the trustor and the trustee. For social human interaction, we consider more about the trustee's subjective and objective properties and the trustor's subjective properties. For economic transactions, we study more about the context for risk management. The context of trust is a very important factor that influences a trust relationship, e.g. the why and when to trust. It specifies any information that can be used to characterize the background or situation of the involved entities. Trust is influenced by many factors, but the impact of different factors could be various in dissimilar contexts.

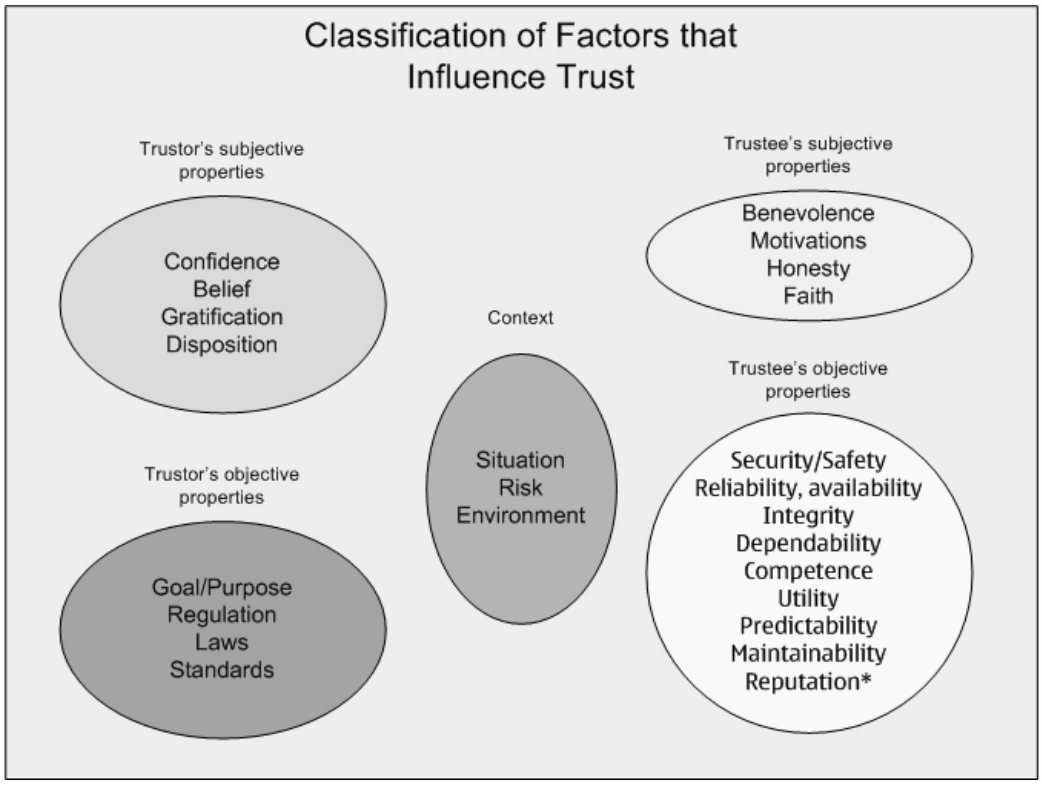

Figure 1: Classification of factors that influence trust

Trust Modeling Technology (Modeling Trust in a Digital Approach)

We introduce the existing trust modeling work in the area of distributed systems, e-commerce and Web services to understand the methodologies used for trust modeling. We will answer questions like: What are the characteristics of trust? What is a trust model? What is trust modeling? What kinds of trust models have been developed and applied in the emerging technologies? Which factors related to trust are considered in the modeling in the literature?

Characteristics of trust. Despite the diversity among the existing definitions of trust, and despite that a precise definition is missing in the literature, there is a large commonality on the properties of trust. Rousseau, Sitkin, Burt, and Camerer (1998) also observed considerable overlap and synthesis in contemporary scholarship on trust. Particularly, the most common characteristics of trust, which play as the important guidelines for trust modeling are:

a) *Trust is directed:* This property says that trust is an oriented relationship between the trustor and the trustee.

b) *Trust is subjective:* Trust is inherently a personal opinion. According to the survey conducted by Grandison and Sloman (2000), trust is considered a personal and subjective phenomenon that is based on various factors or evidence, and that some of those may carry more weight than others. Trust is different for each individual in a certain situation.

c) *Trust is context-dependent:* In general, trust is a subjective belief about an entity in a particular context.

d) *Trust is measurable:* Trust values can be used to represent the different degrees of trust an entity may have in another. "Trust is measurable" also provides the foundation for trust modeling and computational evaluation.

e) *Trust depends on history:* This property implies that past experience may influence the present level of trust.

f) *Trust is dynamic:* Trust is usually non-monotonically changed with time. It may be refreshed or revoked periodically, and must be able to adapt to the changing conditions of the environment in which the trust decision was made. Trust is sensitive to be influenced due to some factors, events, or changes of context. In order to handle this dynamic property of trust, solutions should take into account the notion of learning and reasoning. The dynamical adaptation of the trust relationship between two entities requires a sophisticated trust management approach (Grandison and Sloman, 2000).

g) Trust is conditionally transferable: Information about trust can be transmitted/received along a chain (or network) of recommendations. The conditions are often bound to the context and the trustor's objective factors.

h) Trust can be a composite property: "trust is really a composition of many different attributes: reliability, dependability, honesty, truthfulness, security, competence, and timeliness, which may have to be considered depending on the environment in which trust is being specified" (Grandison and Sloman, 2000, pp. 3). Compositionality is an important feature for making trust calculations.

Trust modeling. What is a trust model? The method to specify, evaluate and set up trust relationships amongst entities for calculating trust is referred as the trust model. Trust modeling is the technical approach used to represent trust for the purpose of digital processing.

One of the earliest formalizations of trust in computing systems was done by Marsh (1994). In his approach, he integrated the various facets of trust from the disciplines of economics, psychology, philosophy and sociology. Since then, many trust models have been constructed for various computing paradigms such as ubiquitous computing, P2P networks, and multi-agent systems. In almost all of these studies, trust is accepted as a subjective notion by all researchers, which brings us to a problem: how to measure trust? Translation of this subjective concept into a machine readable language is the main objective needed to be solved. Rahman and Hailes (2000) proposed a trust model based on the work done by Marsh (2000). Their trust model focuses on online virtual communities where every agent maintained a large data structure representing a version of global knowledge about the entire network. Gil and Ratnakar (2002) described a feedback mechanism that assigns credibility and reliability values to sources based on the averages of feedback received from individual users.

Regarding the trust modeling, there are various methodologies can be applied for different purposes. Some trust models are based on cryptographic technologies, e.g. Public Key Infrastructure (PKI) played as the foundation in a trust model (Perlman, 1999). A big number of trust models are developed targeting at some special trust properties, such as reputations, recommendations and risk studied by Xiong and Liu (2004) and Liang and Shi (2005). Seldom, they support multi-property of trust that is needed to take into account the factors like multiple objective factors of the trustee and context. Many trust models have been constructed for various computing paradigms such as GRID computing, ad hoc networks, and P2P systems. Those models use computational, linguistic or graphical methods. For example, Maurer (1996) described an entity's opinion about the trustworthiness of a certificate as a value in the scope of [0, 1]. Theodorakopoulos and Baras (2006) used a two-tuple in $[0, 1]^2$ to describe a trust opinion. In Jøsang (1999), the metric is a triplet in $[0, 1]^3$, where the elements in the triplet represent belief, disbelief, and uncertainty, respectively. Abdul-Rahman and Hailes (2000) used discrete integer numbers to describe the degree of trust. Then, simple mathematic, such as minimum,

maximum, and weighted average, is used to calculate unknown trust values through concatenation and multi-path trust propagation. Jøsang and Ismail (2002) and Ganeriwal and Srivastava (2004) used a Bayesian model to take binary ratings as input and compute reputation scores by statistically updating beta probability density functions. Linguistic trust metrics were used for reasoning trust with provided rules by Manchala (2000). In the context of the "Web of Trust", many trust models (e.g. Reiter and Stubblebine, 1998) are built upon a graph where the resources/entities are nodes and trust relationships are edges.

One promising approach of trust modeling aims to conceptualize trust based on user studies through a psychological or sociological approach (e.g. a measurement scale). This kind of research aims to prove the complicated relationships among trust and other multiple factors in different facets. Two typical examples are the initial trust model proposed by McKnight, Choudhury, and Kacmar (2002) that explained and predicted customer's trust towards an e-vender in an e-commerce context, and the Technology Trust Formation Model (TTFM) studied by Li, Valacich, and Hess (2004) to explain and predict people's trust towards a specific information system. Both models used the framework of the theory of reasoned action (TRA) created by Fishbein and Ajzen (1975) to explain how people form initial trust in an unfamiliar entity, and both integrated important trusting antecedents into this framework in order to effectively predict people's trust. For other examples, Gefen (2000) proved that familiarity builds trust; Pennington, Wilcox, and Grover (2004) tested that one trust mechanism, vendor guarantees, has direct influence on system trust; Bhattacherjee (2002) studied three key dimensions of trust: trustee's ability, benevolence and integrity; Pavlou and Gefen (2004) explained that institutional mechanisms engender buyer's trust in the community of online auction sellers. The trust models generated based on this approach are generally linguistic or graphic. They do not quantify trust for machine processing purposes. Therefore, the achieved results could only help people understanding trust more precisely in order to work out a design guideline or an organizational policy towards a trustworthy digital system or a trustworthy user interface. Although little work has been conducted to integrate psychological, sociological and technological theories together, we believe, however, the psychological and sociological study results could further play as practical foundations of computational trust – modeling trust for a digital processing purpose,.

Modeling trust in a digital way is important in a distributed digital system in order to automatically manage trust. Although a variety of trust models are available, it is still not well understood what fundamental criteria the trust models must follow. Without a good answer to this question, the design of trust models is still at an empirical stage and can never reach the expectation to simulate social trust to a satisfying degree. Current work focuses on concrete solutions in special systems. We would like to advocate that the trust model should reflect the characteristics of trust, consider the factors that influence the trust, and thus support the trust management in a feasible way.

Despite the variety of trust modeling methods, a common approach can be found in a number of publications regarding computational trust, e.g. Xiong and Liu (2004), Theodorakopoulos and Baras (2006), Song, Hwang, Zhou, and Kwok (2005), Liu, Joy, and Thompson (2004), and Sun, et al. (2006). This approach is applied by firstly presenting an understanding of the characteristics of trust, principles or axioms, then modeling them in a mathematical way, and further applying the model into trust evaluation or trust management for a specific issue.

Taxonomy of trust models. The trust model aims to process and/or control trust using digital methods. Most of the modeling work is based on the understanding of trust characteristics and

considers some factors influencing trust. The current work covers a wide area including ubiquitous computing, distributed systems, multi-agent systems, Web services, e-commerce, and component software. The discussed trust models can be classified into categories according to different criteria, as shown in Table 2.

Table 2: Taxonomy of trust models

Criteria of classification	**Categories**		**Examples**
Based on the method of modeling	Models with linguistic description		Blaze, Feigenbaum, and Lacy (1996) and Tan and Thoen (1998)
	Models with graphic description		Reiter and Stubblebine (1998)
	Models with mathematic description		Xiong and Liu (2004) and Sun, Yu, Han, and Liu (2006)
Based on modeled contents	Single-property modeling		Xiong and Liu (2004) and Sun, Yu, Han, and Liu (2006)
	Multi-property modeling		Zhou, Mei, and Zhang (2005), Wang and Varadharajan (2005), and Yan and MacLaverty (2006)
Based on the expression of trust	Models with binary rating		
	Models with numeral rating	Continuous rating	Maurer (1996) and Xiong and Liu (2004)
		Discrete rating	Liu, Joy, and Thompson (2004)
Based on the dimension of trust expression	Models with single dimension		Maurer (1996) and Xiong and Liu (2004)
	Models with multiple dimensions		Theodorakopoulos and Baras (2006) and Jøsang (1999)

Current research status. Trust is influenced by reputations (i.e. the public evidence of the trustee), recommendations (i.e. a group of entities' evidence on the trustee), the trustor's past experiences and context (e.g. situation, risk, time, etc.). Most of work focused on a singular trust value or level calculation by taking into account the previous behavior of the trustee. The reputations, the recommendations and the trustor's own experiences are assessed based on the quality attributes of the trustee, the trust standards of the trustor and the local context for making a trust or distrust conclusion. A number of trust models support the dynamics of trust. So far, some basic elements of context are considered, such as time, context similarity, etc. The time element has been considered in many pieces of work, such as Wang and Varadharajan (2005) and Xiong and Liu (2004). For peer-to-peer systems, Sarkio and Holtmanns (2007) proposed a set of functions to produce a tailored trustworthiness estimation, which takes into account factors like age of reputation, value of transaction, frequency of transactions, reputation of the reputation giver etc. However, no existing work gives a common consideration on all factors that influence trust in a generic digital environment, especially those subjective factors of the trustor and the trustee, as shown in Figure 1. It is still a challenge to digitally model the subjective factors related to the trustor and the trustee, especially when the trustor or the trustee is a person.

Mechanisms for Trust Management (Applying and Deploying Trust Models)

About the following questions will be addressed in this part: "What is trust management? What does trust management do? Why is trust management needed in the emerging technologies? What is the current research status of trust management?"

As defined in Grandison and Sloman (2000), trust management is concerned with: collecting the information required to make a trust relationship decision; evaluating the criteria related to the trust relationship as well as monitoring and reevaluating existing trust relationships; and automating the process. Due to the amount of data collected and processed in the digital environment, the definition should be extended to accommodate support for automatic processing in order to provide a system's trustworthiness. Yan and MacLaverty (2006) proposed that autonomic trust management includes four aspects and these four aspects are processed in an automatic way:

- *Trust establishment:* The process for establishing a trust relationship between a trustor and a trustee.

- *Trust monitoring:* The trustor or its delegate monitors the performance or behaviour of the trustee. The monitoring process aims to collect useful evidence for trust assessment of the trustee.

- *Trust assessment:* The process for evaluating the trustworthiness of the trustee by the trustor or its delegate. The trustor assesses the current trust relationship and decides if this relationship is changed. If it is changed, the trustor will make decision which measure should be taken.

- *Trust control and re-establishment:* If the trust relationship will be broken or is broken, the trustor will take corresponding measures to control or re-establish the trust relationship.

As we can see from the above, trust management can be achieved through trust modeling and evaluation.

Reputation systems. There are various trust management systems in the literature and practice. A category of large practical importance is reputation based trust management system. Trust and reputation mechanisms have been proposed in various fields such as distributed computing, agent technology, grid computing, economics and evolutionary biology. Reputation-based trust research stands at the crossroads of several distinct research communities, most notably computer science, economics, and sociology.

As defined by Aberer and Despotovic (2001), *reputation* is a measure that is derived from direct or indirect knowledge on earlier interactions of entities and is used to assess the level of trust an entity puts into another entity. Thus, reputation based trust management (or simply reputation system) is a specific approach to evaluate and control trust.

Reputation schemes can be classified into two different categories depending on what sort of reputation they utilize. Global reputation is the aggregation of all available assessments by other entities that have had interactions with the particular entity, and thus it has an *n-to-1 relationship*. On the other hand, the local reputation of an entity is each entity's own assessment based on past history of interaction with the particular entity, thus it is a *1-to-1 relationship*. This reflects the social situation that a person trusts another one, because "they are good friends".

Several representative P2P reputation systems currently exist, although the list we present is by no means exhaustive. The eBay and PeerTrust systems focus on trust management in securing commodity exchanges in e-commerce applications, as does the FuzzyTrust system by Song, Hwang, Zhou, and Kwok (2005). Other systems focus on generic P2P applications such as P2P file sharing and Web service-based sharing platforms.

The eBay (www.ebay.com) user feedback system described by Resnick and Zeckhauser (2002) is by far the simplest and most popular trust-management system, and is specifically tailored for e-auction applications. It applies a centralized database to store and manage the trust scores. Data is open to the general public, so a newcomer can easily obtain a peer score. It's a hybrid P2P system using both distributed client resources and centralized servers. This system tries to be user friendly by providing a limited amount of data to a user, but on the other hand the provided and processed information is not complete and does not provide a "full picture".

Singh and Liu (2003) presented Trustme, a secure and anonymous protocol for trust. The protocol provides mutual anonymity for both a trust host and a trust querying peer. Guha and Kumar (2004) developed an interesting idea about the propagation of distrust. In addition to maintaining positive trust values for peers, the system also allows the proactive dissemination of some malicious peers' bad reputations. Buchegger and Le Boudec (2004) designed a distributed reputation system using a Bayesian approach, in which the second-hand reputation rating is accepted only when it is not compatible with the primary rating.

Several universities are working on the research projects involving trust management in P2P applications. Xiong and Liu (2004) developed the PeerTrust model. Their model is based on a weighted sum of five peer feedback factors: *peer records, scope, credibility, transaction context,* and *community context.* PeerTrust is fully distributed, uses overlay for trust propagation, public-key infrastructure for securing remote scores, and prevents peers from some malicious abuses.

Kamvar, Schlosser, and Garcia-Molina (2003) proposed the EigenTrust algorithm, which captures peer reputation in the number of satisfactory transactions and then normalizes it over all participating peers. The algorithm aggregates the scores by a weighted sum of all raw reputation scores. The fully distributed system assumes that pre-trusted peers exist when the system is initiated. It uses majority voting to check faulty reputation scores reported.

Liang and Shi (2005) proposed the TrustWare system (retrieved from http://mist.cs.wayne.edu/trustware.html), a trusted middleware for P2P applications. Their approach consists of two models: the Multiple Currency Based Economic model (M-CUBE) and the Personalized Trust model (PET). The M-CUBE model provides a general and flexible substrate to support high-level P2P resource management services. PET derives peer trustworthiness from long-term reputation evaluation and short-term risk evaluation.

Sherwood and Bhattacharjee (2003) proposed in the Nice project a scheme for trust inference in P2P networks. The trust inference consists of two parts for local trust inference and distributed search. After each transaction, the system generates cookies to record direct trust between peers. It also uses trust graphs to infer transitive trust along a peer chain.

Credence is a robust and decentralized system for evaluating the reputation of files in a P2P file sharing system (Retrieved from http://www.cs.cornell.edu/people/egs/credence/index.html). Its goal is to enable peers to confidently gauge *file authenticity*, the degree to which the content of a file matches its advertised description. At the most basic level, Credence employs a simple, network-wide voting scheme where users can contribute positive and negative evaluations of files. On top of this, a client uses statistical tests to weight the importance of votes from other peers. It allows the clients to share selected information with other peers. Privacy is ensured by not collecting or using any personally identifiable information in any way in the protocol. Each Credence-equipped client is supplied with a unique, randomly generated key pair that is not bound to any personal information for use in cryptographic operations.

Meanwhile, European Union (EU) project SECURE investigated the design of security mechanisms for pervasive computing based on the human notion of trust. It addresses how

entities in unfamiliar pervasive computing environments can overcome initial suspicion to provide secure collaboration (Cahill, V. et al. 2003). Another EU project Trust4All aims to build up trustworthy middleware architecture in order to support easy and late integration of software from multiple suppliers and still have dependable and secure operations in the resulting system (Retrieved from https://nlsvr2.ehv.compus.philips.com/).

Requirements of trust for ad hoc networks. More dimensions are needed to secure the communications in wireless mobile ad hoc networks. Balakrishnan and Varadharajan (2005) demonstrated the issues that might creep out in the security design, when a cryptographic technique alone is involved. They also suggested how to counter those issues through the combination of trust management with cryptographic mechanisms. Moreover, they proposed the need to introduce the notion of heterogeneity resource management in the security design to address the divergence among the nodes, which can be taken advantage to diminish the packet drop attacks. To handle the dynamic nature of the medium, the authors proposed that the design of secure mobile ad hoc networks should envisage including trust management as another dimension apart from the cryptographic mechanisms. In addition, inclusion of trust management alone cannot guarantee secure communication due to some persisting issues such as packet dropping. Therefore, the resource should be also considered in order to provide a trustworthy system.

Trust Evaluation Mechanisms (Methodologies for Trust Decision)

Trust evaluation is a technical approach of representing trustworthiness for digital processing, in which the factors influencing trust will be evaluated by a continuous or discrete real number, referred to as a trust value. A trust evaluation mechanism aims to provide supporting information for the actual trust decision of an entity for managing trust. Embedding a trust evaluation mechanism is a necessity to provide trust intelligence in future computing devices.

The trust evaluation is the main aspect in the research for the purpose of digitalizing trust for computer processing. A number of theories about trust evaluation can be found in the literature. For example, Subjective Logic was introduced by Jøsang (2001). It can be chosen as trust representation, evaluation and update functions. The Subjective Logic has a mathematical foundation in dealing with evidential beliefs rooted in the Shafer's theory and the inherent ability to express uncertainty explicitly. The trust valuation can be calculated as an instance of the opinion in the Subjective Logic. An entity can collect the opinions about other entities both explicitly via a recommendation protocol and implicitly via limited internal trust analysis using its own trust base. It is natural that the entity can perform an operation in which these individual opinions can be combined into a single opinion to allow relatively objective judgment about other entity's trustworthiness. It is desirable that such a combination operation shall be robust enough to tolerate situations where some of the recommenders may be wrong or dishonest. Other situation with respect to trust valuation combination includes combining the opinions of different entities on the same entity together; aggregation of an entity's opinion on two distinct entities together with logical AND support or with logical OR support. (The description and demo about the Subjective Logic can be retrieved from http://sky.fit.qut.edu.au/~josang/sl/demo/Op.html.)

But the Subjective Logic is a theory about opinion that can be used to represent trust. Its operators mainly support the operations between two opinions. It doesn't consider context support, such as time based decay, interaction times or frequency, and trust standard support like importance weights of different trust factors. Concretely, how to generate an opinion on a recommendation based on credibility and similarity and how to overcome attacks of trust

evaluation are beyond the Subjective Logic theory. The solutions of these issues need to be further developed in practice.

Fuzzy Cognitive Maps (FCM) developed by Kosko (1986) could be regarded as a combination of Fuzzy Logic and Neural Networks. In a graphical illustration, the FCM seems to be a signed directed graph with feedback, consisting of nodes and weighted arcs. Nodes of the graph stand for the concepts that are used to describe the behavior of the system and they are connected by signed and weighted arcs representing the causal relationships that exist between the concepts, as depicted in Figure 2.

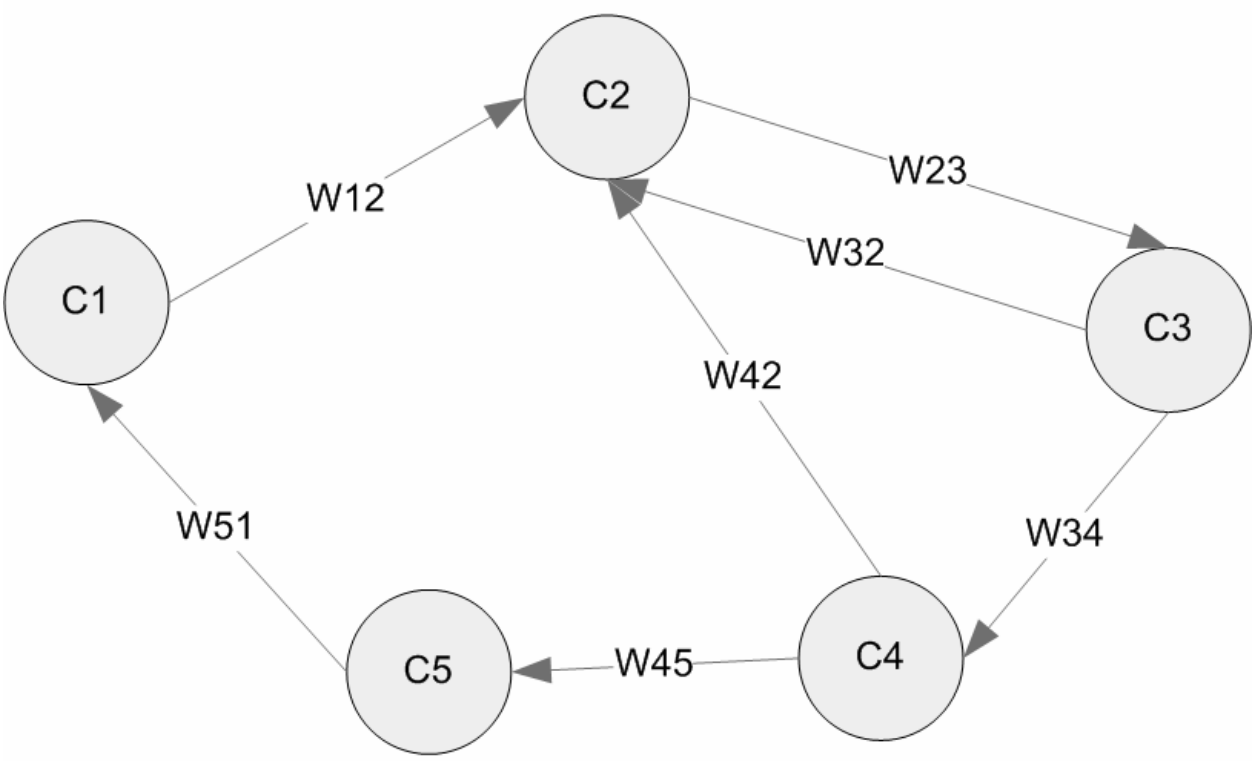

Figure 2: A simple Fuzzy Cognitive Map

The FCM can be used for evaluating trust. In this case, the concept nodes are trustworthiness and factors that influence trust. The weighted arcs represent the impact of the trust influencing factors to the trustworthiness. These weighted arcs allow putting weight on the trust influencing factors. The FCM is convenient and practical for implementing and integrating trustworthiness and its influencing factors. In addition, Song, Hwang, Zhou, and Kwok (2005) made use of fuzzy logic approach to develop an effective and efficient reputation system.

Theodorakopoulos and Baras (2006) introduced Semiring. It views the trust inference problem as a generalized shortest path problem on a weighted directed graph *G(V, E)* (*trust graph*). The vertices *V* of the graph are the users/entities in the network. A weighted edge that belongs to *E* from vertex *i* to vertex *j* corresponds to the *opinion* that the trustor *i* has about the trustee *j*. The weight function is $l(i,j)$: $V \times V \rightarrow S$, where *S* is the opinion space. Each opinion consists of two numbers: the *trust* value, and the *confidence* value. The former corresponds to the trustor's estimate of the trustee's trustworthiness. The confidence value corresponds to the accuracy of the trust value assignment. Since opinions with a high confidence value are more useful in making trust decisions, the confidence value is also referred to as the *quality or reliability* of the opinion. The space of opinions can be visualized as a rectangle (*ZERO_TRUST,*

MAX_TRUST)×*(ZERO_CONF, MAX_CONF*) in the Cartesian plane. They don't treat distrust or negative confidence, but these could be accommodated by rescaling *S*.

A *Semiring* is an algebraic structure $(S,\oplus,\otimes)$, where S is a set, and $\oplus$, $\otimes$ are binary operators. $\oplus$, $\otimes$ are associative and $\oplus$ is commutative. $\oplus$ and $\otimes$ can be used to aggregate opinions along the paths from the trustor to the trustee together. Concretely, $\otimes$ is used to calculate the opinion along a path from the trustor to the trustee, while $\oplus$ is applied to compute the opinion as a function of all paths from the trustor to the trustee. Theodorakopoulos and Baras (2006) gave the formula of $\oplus$ and $\otimes$ regarding path Semiring and distance Semiring.

Sun, Yu, Han, and Liu (2006) presented an information theoretic framework to quantitatively measure trust and model trust propagation in the ad hoc networks. In the proposed framework, trust is a measure of uncertainty with its value represented by entropy. The authors develop four Axioms that address the basic understanding of trust and the rules for trust propagation. Based on these axioms two trust models are introduced: entropy-based model and probability-based model, which satisfy all the axioms. Xiong and Liu (2004) introduced five trust parameters in PeerTrust. By formalizing these parameters, they presented a general trust metric that combines these parameters in a coherent scheme. This model can be applied into a decentralized P2P environment. It is effective against dynamic personality of peers and malicious behaviors of peers.

DIGITAL MANAGEMENT OF TRUST

Issues, Controversies and Problems

The rapid evolution of the digital environment and emerging technologies creates a number of issues related to trust.

E-commerce. Electronic commerce and services are revolutionizing the way we conduct our personal and organizational business. And this trend will be extended to mobile domain. But it is very hard to build up a long-term trust relationship between all involved parties: manufactures, service providers, application providers, access providers and end users. Different legislation areas and distrust in the applicable legal frameworks of transaction partners make the creation of a trust foundation necessary for the electronic transaction quite challenging. This could be a major obstacle that retards the further development of e-commerce.

Hoffman, Novak, and Peralta (1999) pointed out that the reason more people have yet to shop online or even provide information to Web providers in exchange for access to information is the fundamental lack of faith between most businesses and consumers on the Web. Almost 95% of Web users have declined to provide personal information to Web sites when asked because they are not clear how the personal data will be used and they feel there is no way for them to control over secondary use of their personal information (Hoffman, Novak, and Peralta, 1999). In addition, differently from traditional commerce, uncertainty about product quality, i.e. information asymmetry is always a problem for consumers in an online environment (Ba and Pavlou, 2002). Lack of consumer trust is a critical impediment to the success of e-commerce. Ultimately, the most effective way for commercial Web providers to develop profitable exchange relationships with online customers is to earn their trust. Trust thus becomes a vital factor influencing the final success of e-commerce.

Digital distributed networking and communications. On the other hand, new networking is raising with the fast development of Mobile Ad hoc Networks (MANET) and local wireless communication technologies. Boundaries between traditional computers, laptops, mobile phones,

Personal Digital Assistants (PDA) and consumer electronics devices dissolve. It is more convenient for mobile users to communicate in their proximity to exchange digital information in various circumstances. However, the special characteristics of the new networking paradigms (e.g. dynamically changed topology) introduce additional challenges on security. The ad hoc networks are generally more prone to physical security threats than conventional networks, due to their lack of any security infrastructure support. Security approaches used for fixed networks are not feasible due to the salient characteristics of the ad hoc networks. The root of the threats is originated from the lack of trust among network nodes.

In addition, new P2P computing technology has emerged as a significant paradigm for providing distributed services, in particular collaboration for content sharing and distributed computing. Generally, a P2P system consists of a decentralized and self-organizing network of autonomous devices that interact as peers. Each peer acts as both client and server to share its resources with other peers. However, this computing paradigm suffers from several drawbacks that obstruct its wide adoption. Lack of trust between peers is one of the most serious issues, which causes security challenges in the P2P systems. Building up trust collaboration among the system peers is a key issue to overcome, especially in the mobile environment.

GRID computing systems have attracted research communities in recent years. This is due to the unique ability of marshalling collections of heterogeneous computers and resources, enabling easy access to diverse resources and services that could not be possible without a GRID model. The context of GRID computing does introduce its own set of security challenges, as user(s) and resource provider(s) can come from mutually distrusted administrative domains and either participant can behave maliciously.

User-device or user-system interaction. Most current digital systems are designed based on the assumptions that the user trusts his/her device fully; or the user has to trust a service provider. Generally, the current systems are not designed to be configured by user with regard to their trust preferences. As can be seen from the above study, trust evaluation based management technology has been proposed to overcome the challenge of trust and security in distributed systems and Internet e-commerce However, the human-machine interaction in order to support trust management, especially in mobile domain, has still many open research questions. Embedding personal criteria of trust regarding different events into the device or system requires interaction between the end user and his/her devices. This would require friendly user interface for the device to collect useful information for trust evaluation and present the evaluation results in a comprehensive manner to the user. It also provides a technical challenge to design an effective trust management system that is light weight with regard to memory management, process observation and data mining.

Privacy support. User data privacy is hard to control once the personal data is released into digital format. New customized services require detailed user information like location, preferences or general behavior profiles. People expect such a privacy control service that only trusted parties can get specified personal information. The user-friendly administration of this control is a tough challenge especially for the mobile systems with a limited user interface even through taking into account the latest privacy visualization approaches for the mobile environment (Hjelm and Holtmanns, 2006).

How to solve these issues described above depends on better understanding of trust, trust modeling and management technologies.

Solutions and Recommendations

Solutions for the trust issues of e-commerce. Trust management is introduced to evaluate trust for reduced risk. Tan and Thoen (1998) specified a generic model of transaction trust for e-commerce as party trust supplemented with control trust. It provides a generic model of transaction trust for e-commerce. This model is based on separating the mostly subjective party trust and mostly objective control trust. The transaction trust consists of the sum of the party trust and the control trust. If the level of the transaction trust is not sufficient, then the party trust should be possibly complemented by the control trust in order to reach a required level. This theory was further developed to build up online trust between trading parties in a first trade situation through a trust matrix model.

Manchala (2000) described metrics and models for the measurement of trust variables and fuzzy verification of transactions. The trust metrics help preserve system availability by determining risk on transactions. Several variables (such as cost of transaction, transaction history, customer loyalty, indemnity, spending pattern, and system specific) on which trust depends are used to define trust. These variables in turn influence actions taken by a transacting entity (e.g. verification, security level decision, and authorization). Certain parameters, such as time and location, modify trust actions. In addition, Manchala pointed out that the existing e-commerce protocols have not been equipped with mechanisms to protect a vendor from a customer who makes a fraudulent payment or a customer from a vendor who supplies low quality or garbage goods. In other words, these protocols need to be equipped with suitable trust mechanisms and they should be strengthened by adding a non-reputable context to the transaction protocol. In an e-commerce transaction, mutual trust should exist between a vendor and a customer with several intermediaries involved in the transaction. In practical scenarios, e-Bay, for example, offers a safeguard service, that ensures the payment and the satisfactory delivery of the goods, but this service is not without costs.

The game theory-based research lays the foundation for online reputation systems research and provides interesting insight into the complex behavioral dynamics. Most of the game theoretic models assume that stage game outcomes are publicly observed. Online feedback mechanisms, in contrast, rely on private (pair-wise) and subjective ratings of stage game outcomes. Dellarocas (2003) introduced two important considerations, the incentive for providing feedback and the credibility or the truthfulness of the feedback.

Khare, R., & Rifkin, A. (1998) presented pragmatic details of Web-based trust management technology for identifying principals, labeling resources, and enforcing policies. It sketched how trust management might be integrated into Web applications for document authoring and distribution, content filtering, and mobile code security. By measuring today's Web protocols, servers, and clients, the authors called for stakeholders' support in bringing automatable trust management to the Web.

The reputation systems play an important role to evaluate the trustworthiness of transaction parties. A number of reputation systems and mechanisms were proposed for online environments and agent systems. Pujol, Sanguesa, and Delgado (2002) applied network flow techniques and proposed a generalized algorithm that extracts the reputation in a general class of social networks. Jøsang and Ismail (2002) and Jøsang and Tran (2003) developed and evaluated the beta reputation system for electronic markets by modeling reputation as posterior probability given a sequence of experiences. Among other things, they showed that a market with limited duration rather than infinite longevity of transaction feedback provides the best condition. Sabater and Sierra (2002) proposed Regret system and showed how social network analysis can be used in the reputation system. Sen and Sajja (2002) proposed a word-of-mouth reputation

algorithm to select service providers. Their focus was on allowing querying agent to select one of the high-performance service providers with a minimum probabilistic guarantee. Yu and Singh (2000) developed an approach for social reputation management and their model combines agents' belief ratings using combination schemes similar to certainty factors. The reputation ratings are propagated through neighbors. Zacharia and Maes (2000) proposed an approach that is an approximation of game-theoretic models and studied the effects of feedback mechanisms on markets with dynamic pricing using simulation modeling.

A few proposals specifically attempted to address the issue of quality or credibility of the feedback. Chen and Singh (2001) differentiated the ratings by the reputation of raters that is computed based the majority opinions of the rating. Adversaries who submit dishonest feedback can still gain a good reputation as a rater in a method simply by submitting a large number of feedback and becoming the majority opinion. Dellarocas (2000) proposed mechanisms to combat two types of cheating behaviors when submitting feedbacks. The basic idea is to detect and filter out the feedbacks in certain scenarios using cluster-filtering techniques. The technique can be applied into feedback-based reputation systems to filter out the suspicious "fake" ratings before an actual aggregation. Miller, Resnick, and Zeckhauser (2002) proposed a mechanism, based on budget balanced payments in exchange for feedbacks, which provides strict incentives for all agents to tell the truth. This provides yet another approach to the problem of feedback trustworthiness. However, such a mechanism is vulnerable to malicious collusion. The development of effective mechanisms for dealing with collusive manipulations of online reputations systems is currently an active area of research.

On the other side, Salam, Iyer, Palvia, and Singh (2005) explored a framework to highlight the importance of nurturing consumer trust in the context of e-commerce. In particular, the authors pointed that the technical approaches to establish credibility and integrity are necessary but not sufficient for creating the long-term trusting relationships between consumers and online businesses. Web vendors must align both their long-term and short-term relationships with consumers and develop interventions to inspire consumer beliefs that affect their attitudes, intentions, and dependence, and ultimately their willingness to spend money. The Web vendors must address the factors affecting different belief classes to establish the trustworthiness of their organizations. They need a long-term approach to manage trust and generate a positive consumer experience from each and every Internet transaction. Quite a number of studies attempted to seek trust building factors and their relationships in order to propose guidelines or policies for designing a trustworthy e-commerce solution, for example, Jones, Wilikens, Morris, and Masera (2000), Rutter (2001), McKnight, Choudhury, and Kacmar (2002), Li, Valacich, and Hess (2004), Gefen (2000), Pennington, Wilcox, and Grover (2004), Bhattacherjee (2002) and Pavlou and Gefen (2004). As we can see from the above, technologies and policies are in parallel influencing and enhancing trust management.

Solutions for distributed systems. Trust modeling and management can be applied to enhance security, dependability and other quality attributes of a system or a system entity. Main usage of trust management can be summarized below:

- Detecting malicious entity in a system;
- Helping in decision making in system processing;
- Selecting the best entity from a number of candidates, e.g. selecting the best route node or the best path in MANET;
- Benefiting on system optimization. For example, if an entity is trusted, some procedures can be saved, which could benefit the efficiency of a system.

- Improving Quality of Services through applying trust management technology in a system.

So far, the trust evaluation and management technology have been studied and developed in many areas, such as distributed systems: P2P, Ad hoc, GRID; E-commerce, Web services; and software engineering. For example, P2P library, resource management in GRID, security enhancement in GRID computing, trusted Ad hoc routing and component software system configurations. We have introduced many of them in Section 2.3.

Tajeddine, Kayssi, Chehab, and Artail (2005) proposed a comprehensive reputation based trust model for distributed system. This approach requires that a host asks about the reputation of a target host that it wants to interact with. It calculates a reputation value based on its previous experiences and the gathered reputation values from other hosts, and then it decides whether to interact with the target host or not. The initiator also evaluates the credibility of hosts providing reputation values by estimating the similarity, the activity, the popularity, and the cooperation of the queried host. Moreover, each host uses different dynamic decay factors that depend on the consistency of the interaction results of a certain host.

Common opinions can be summarized based on the literature study. For a distributed system, trust modeling and evaluation can be used for improving system security and reliability. The trust of a trustor on a trustee is based on the trustor's past experience in the same or similar context, and recommendations or reputations generated from the experiences of other system entities. The contributions of the recommendations and the trustor's experiences to the trust value calculation are influenced by their age or time. The recommendations' contribution is also influenced by such factors as the trustor's opinion on the recommenders, distance (e.g. hops between the trustor and the recommender in ad hoc networks), and so on. Taking some detailed examples of policies for trust evaluation,

- Trust value is no bigger than trust value generated by trustor's experiences or recommendations;
- Latest information from experiences and recommendations will contribute more the calculation of trust value.

Furthermore, we summarize the factors considered in trust modeling:

- Recommendations, reputations, feedback from other entities (based on their experiences)
- Personal or local experience and its influencing factor (e.g. the time of the experience)
- Trust (credibility) on recommendations/reputations of the trustor
- Context factors (e.g. time, distance, transaction context, community context)
- Policy factors, i.e. the trustor's standards with regard to trust (e.g. accepted level of recommendations)

The above factors are generally aggregated through weighting. The weighting has some dependencies, for example, similarity, activity, popularity, and cooperation of a certain entity.

However, most modeling aims to support trust evaluation for decision making. Little considers trust control or management, for example, how to maintain trust for a period of time based on the evaluation. Trust management is more than trust evaluation, especially in an open computing platform, where autonomic trust management is becoming an important research topic.

Solutions for user-device or user-system interaction. A number of trusted computing projects have been conducted in the literature and industry. For example, Trusted Computing Group (TCG) defines and promotes open standards for hardware-enabled trusted computing and

security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices. TCG specified technology enables more secure computing environments without compromising functional integrity, privacy, or individual rights. It aims to build up a trusted computing device on the basis of a secure hardware chip – Trusted Platform Module (TPM). In short, the TPM is the hardware that controls the boot-up process. Every time the computer is reset, the TPM steps in, verifies the Operating System (OS) loader before letting boot-up continue. The OS loader is assumed to verify the Operating System. The OS is then assumed to verify every bit of software that it can find in the computer, and so on. The TPM allow all hardware and software components to check whether they have woken up in trusted states. If not, they should refuse to work. It also provides a secure storage for confidential information. In addition, it is possible for the computer user to select whether to boot his/her machine in a trusted computing mode or in a legacy mode.

eBay, Amazon, etc. famous internet services show the recommendation level of sellers and products based on the feedback accumulated. Credence employs a simple, network-wide voting scheme where users can contribute positive and negative evaluations of files. On top of this, a client uses statistical tests to weight the importance of votes from other peers. And finally, Credence allows clients to extend the horizon of information by selectively sharing information with other peers.

In order to design a trustworthy system, a number of user studies provide results on how to design a trustworthy user interfaces, especially for the recommendation systems. For example, Herlocker, Konstan, and Riedl (2000) studied explanation's aid on user trust regarding Automated Collaborative Filtering (ACF) - a technological recommendation approach based on the similarity of interest). It addressed explanation interfaces for the ACF systems – *how* they should be implemented and *why* they should be implemented. It presented that experimental evidence shows that providing explanations can improve the acceptance of the ACF systems.

As we have discussed, trust is a subjective topic. A system is trusted if and only if its users trust it. But little work practiced to formalize user-device or user-system interaction in order to extract the user's standards, as well as adaptively provide information about trust status to the user, particularly if the device is portable with a limited screen.

Privacy support. Trust modeling and management can not only enhance security, but also support privacy. The term *privacy* denotes the ability of an entity to determine whether, when, and to whom information is to be released. With the trust modeling and evaluation, it is helpful to determine above 'whether', 'when' and 'to whom'. However, it lacks discussion on how to enhance privacy through trust management in the literature.

Limitations and Further Discussion

Trust modeling and management remain an active research area in recent years. Trust is today's fashion in security (Gollmann, 2007). However, many interesting research issues are yet to be fully explored. We summarize some of them for interested readers.

As discussed above, it lacks a widely accepted trust definition across multiple related disciplines. This could cause a comprehensive trust model missing in the literature. Perhaps it is impossible to have such a model that can be applied in various situations and systems. Diverse definitions could make normal people confused. This would make it hard for them to understand a trust management solution.

Secondly, it lacks general criteria to assess the effectiveness of a trust model and a trust management solution in the literature. Why is a trust model trustworthy? Why and how is a trust

management system effective? Most of the existing work overlooked these issues and missed discussions about them. In addition, new attacks or malicious behaviors could also destroy a trust management system. Current prove is still based on empirical and experimental study.

Thirdly, the literature lacks discussions on the competence of trust management. That is when and in which situation trust is possibly or impossibly managed. This is a very interesting and important issue worth our attention, especially for autonomic trust management.

Finally, from the practical point of view, some important issues such as trust/reputation value storage (Li and Singhal, 2007), usability of a trust management system, what is the proper settings of a user's policies for trust decision, and how to extract these policies in a user-friendly way need further exploration.

FUTURE TRENDS

Herein, we provide insights about future and emerging trends on trust modeling and management.

An Integrated 'Soft Trust' and 'Hard Trust' Solution

Theoretically, there are two basic approaches for building up a trust relationship. We name them as a 'soft trust' solution and a 'hard trust' solution. The 'soft trust' solution provides trust based on trust evaluation according to subjective trust standards, facts from previous experiences and history. The 'hard trust' solution builds up trust through structural and objective regulations, standards, as well as widely accepted rules, mechanisms and sound technologies. Possibly, both approaches are applied in a real system. They can cooperate and support with each other to provide a trustworthy system. The 'hard trust' provides a guarantee for the 'soft trust' solution to ensure the integrity of its functionality. The 'soft trust' can provide a guideline to determine which 'hard trust' mechanisms should be applied and at which moment. It provides intelligence for selecting a suitable 'hard trust' solution.

An integrated solution is expected to provide a trust management framework that applies both the 'hard trust' solution and the 'soft trust' solution. This framework should support data collection and management for trust evaluation, trust standards extraction from the trustor (e.g. a system or device user), and experience or evidence dissemination inside and outside the system, as well as a decision engine to provide guidelines for applying effective 'hard trust' mechanisms for trust management purposes.

In addition, how to store, propagate and collect information for trust evaluation and management is seldom considered in the existing theoretical work, but is a relevant issue for deployment. Human-device interaction is also crucial to transmit a user's trust standards to the device and the device needs to provide its assessment on trust to its user. These factors influence the final success of trust management.

Autonomic Trust Management

There is a trend that all the processing for trust management is becoming autonomic. This is benefited from the digitalization of trust model. Since trust relationship is dynamically changed, this requires the trust management should be context-aware and intelligent to handle the context changes. Obviously, it does not suffice to require the trustor (e.g. most possibly a digital system user) to make a lot of trust related decisions because that would destroy any attempt at user friendliness. For example, the user may not be informed enough to make correct decisions. Thus, establishing trust is quite a complex task with many optional actions to take. Rather trust should

be managed automatically following a high level policy established by the trustor. We call such trust management autonomic. Autonomic trust management automatically processes evidence collection, trust evaluation, and trust (re-)establishment and control. We need a proper mechanism to support autonomic trust management not only on trust establishment, but also on trust sustaining. In addition, the trust model itself should be adaptively adjusted in order to match and reflect real system situation. Context-aware trust management and adaptive trust model optimization for autonomic trust management are developing research topics (Campadello et al, 2005 and Yan and Prehofer, 2007).

Cross-Domain Benefit

We can estimate that trust management will not only benefit security, but also other properties of the system, such as privacy, usability, dependability and Quality of Services. Combining trust management with other management tasks (e.g. resource management, power management, identity management, risk management and fault management) or applying it into other areas could produce cross-domain benefits. The outcome system will be a more intelligent system to help users managing their increasing amount of digital trust relationships, while providing also good performance.

CONCLUSIONS

This chapter firstly introduced the perception of trust in the literature. Based on the various definitions of trust, we summarized the factors influencing trust and the characteristics of trust. The trust modeling for digital processing is actually based on the understanding of trust, the influencing factors of trust and its characteristics. From a social concept, trust has become a digital object that can be processed. The research on trust modeling, trust evaluation and trust management that have been conducted in the area of distributed systems and e-commerce was presented. The latest trust management systems model trust using mathematical approaches. Thus, it is possible to conduct digital trust management for the emerging technologies.

Current research on trust modeling mostly focuses on the theoretic study based on empirical and experimental results. It lacks experiences in practice. Most of existing deployed solutions are special system driven. The support of a generic solution for trust management, which also benefits other system properties, is usually not considered. In addition, the user-device interaction with regard to trust management is a topic that needs further study. There are still many interesting research issues requiring full investigation.

Regarding the future trends, we believe an integrated solution is very promising that combines traditional security solution with newly developed trust evaluation based management together. This integrated solution should handle trust management in an automatic way and cooperate with other technologies to offer a better system performance.

REFERENCES

Aberer, K., & Despotovic, Z. (2001). Managing trust in a peer-to-peer information system. Proceedings of the ACM Conference on Information and Knowledge Management (CIKM), USA, pp. 310–317.

Abdul-Rahman, A., & Hailes, S. (2000). Supporting trust in virtual communities. Proceedings of the 33rd Hawaii International Conference on System Sciences, pp. 6007.

Avizienis, A., Laprie, J. C., Randell, B., & Landwehr, C. (2004, January). Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing, vol. 1, Issue 1, pp. 11–33.

Azzedin, F., & Muthucumaru, M. (2004, April). A trust brokering system and its application to resource management in public-resource grids. Proceedings of the 18th International Symposium on Parallel and Distributed Processing, page(s):22.

Ba, S., & Pavlou. P. A. (2002). Evidence of the effects of trust building technology in electronic markets: price premiums and buyer behavior. MIS Quarterly 26(3), 243–268.

Ba, S., Whinston, A., & Zhang, H. (1999). Building trust in the electronic market through an economic incentive mechanism. Proceedings of the International Conference on Information Systems, pp. 208–213.

Balakrishnan, V., & Varadharajan, V. (2005, March). Designing secure wireless mobile ad hoc networks**.** Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA 2005), vol. 2, pp. 5–8.

Bhattacherjee, A. (2002). Individual trust in online firms: scale development and initial test. Journal of Management Information Systems 19(1), 211–241.

Blaze, M., Feigenbaum, J., & Lacy, J. (1996, May). Decentralized trust management. Proceedings of IEEE Symposium on Security and Privacy, pp. 164–173.

Boon, S., & Holmes, J. (1991). The dynamics of interpersonal trust: Resolving uncertainty in the face of risk. In R. Hinde and J. Groebel (Eds.). Cooperation and Prosocial Behavior. Cambridge University Press, Cambridge, UK, pp. 190–211.

Buchegger, S., & Le Boudec, J. Y. (2004). A robust reputation system for P2P and mobile ad-hoc networks. Proceedings of the 2nd Workshop Economics of Peer-to-Peer Systems.

Cahill, V. et al. (July-Sept. 2003). Using trust for secure collaboration in uncertain environments. IEEE Pervasive Computing, 2(3), 52–61.

Campadello, S., Coutand, O., Del Rosso, C., Holtmanns, S., Kanter, T., Räck, C., Mrohs, B., & Steglich, S. (2005). Trust and privacy in context-aware support for communication in mobile groups. Proceedings of Context Awareness for Proactive Systems (CAPS) 2005*,* Helsinki, Finland.

Chen, M., & Singh, J. P. (2001). Computing and using reputations for internet ratings. Proceedings of 3rd ACM Conference on Electronic Commerce.

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: concepts, evolving themes, a model. International Journal of Human-Computer Studies, Trust and Technology, 58(6), 737–758.

Dellarocas, C. (2000). Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior. Proceedings of the 2nd ACM Conference on Electronic Commerce.

Dellarocas, C. (2003). The digitization of word-of-mouth: promise and challenges of online reputation mechanism. Management Science, 49(10).

Denning, DE. (1993). A new paradigm for trusted systems. Proceedings of the IEEE New Paradigms Workshop.

Fishbein, M., & Ajzen, I. (1975). Beliefs, attitude, intention and behavior: an introduction to theory and research. Addison-Wesley, Reading*,* MA.

Gambetta, D. (1990). Can we trust Trust?. Trust: Making and Breaking Cooperative Relations, Basil Blackwell. Oxford.

Ganeriwal, S., & Srivastava, M. B. (2004). Reputation-based framework for high integrity sensor networks. Proceedings of the ACM Security for Ad-Hoc and Sensor Networks, pp. 66–67.
Gefen, D. (2000). E-commerce: the role of familiarity and trust. Omega 28(6), 725–737.
Gil, Y., & Ratnakar, V. (2002, June). Trusting information sources one citizen at a time, Proceedings of the 1st International Semantic Web Conference, Italy.
Gollmann, D. (2007). Why trust is bad for security. Retrieved May 2007, from http://www.sics.se/policy2005/Policy_Pres1/dg-policy-trust.ppt
Grandison, T., & Sloman, M. (2000). A survey of trust in internet applications. IEEE Communications and Survey, 4th Quarter, 3(4), 2–16.
Guha, R., & Kumar, R. (2004). Propagation of trust and distrust. Proceedings of the 13th international conference on World Wide Web, ACM Press, pp. 403–412.
Herlocker, J. L., Konstan, J. A., & Riedl, J. (2000). Explaining collaborative filtering recommendations. Proceedings of the 2000 ACM conference on Computer supported cooperative work.
Hjelm, J., & Holtmanns, S. (2006). Privacy and trust visualization. Computer Human Interaction - CHI 2006 Conference Proceedings and Extended Abstracts, ACM Press, Montréal, Canada.
Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. Communications of the ACM 42(4), 80–87.
Jones, S., Wilikens, M., Morris, P., & Masera, M. (2000). Trust requirements in e-business - a conceptual framework for understanding the needs and concerns of different stakeholders. Communications of the ACM 43(12), 80–87.
Jøsang, A., & Ismail, R. (2002, June). The beta reputation system. Proceedings of the 15th Bled Electronic Commerce Conference.
Jøsang, A. (1999). An algebra for assessing trust in certification chains. Proceedings of the Networking. Distributed System Security Symposium.
Jøsang, A. (2001). A logic for uncertain probabilities. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 9(3), 279–311.
Jøsang, A., & Tran, N. (2003). Simulating the effect of reputation systems on e-markets. Proceedings of the First International Conference on Trust Management.
Kamvar, S. D., Schlosser, M. T., & Garcia-Molina, H. (2003, May). The EigenTrust algorithm for reputation management in P2P networks. Proceedings of the 12th International World Wide Web Conference.
Kosko, B. (1986). Fuzzy cognitive maps. International Journal Man-Machine Studies, 24, 65–75.
Khare, R., & Rifkin, A. (1998). Trust management on the world wide web. First Monday 3(6).
Li, H., & Singhal, M. (2007). Trust management in distributed systems. Computer, 40(2), 45–53.
Li, X., Valacich, J. S., & Hess, T. J. (2004). Predicting user trust in information systems: a comparison of competing trust models. Proceedings of the 37th Annual Hawaii International Conference on System Sciences, 10pp.
Liang, Z., & Shi, W. (2005, January). PET: a PErsonalized Trust model with reputation and risk evaluation for P2P resource sharing. Proceedings of the 38thAnnual Hawaii International Conference on System Sciences, pp. 201b–201b.
Liu, Z., Joy, A. W., & Thompson, R. A. (2004, May). A dynamic trust model for mobile ad hoc networks. Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS 2004), pp. 80–85.

Lee, S., Sherwood, R., & Bhattacharjee, B. (2003). Cooperative peer groups in NICE. Proceedings of the IEEE Conf. Computer Comm. (INFOCOM 03), IEEE CS Press, pp. 1272–1282.

Lin, C., Varadharajan, V., Wang, Y., & Pruthi, V. (2004). Enhancing GRID security with trust management. Proceedings of the IEEE International Conference on Services Computing (SCC 2004), pp. 303–310.

Manchala, D.W. (2000). E-commerce trust metrics and models. IEEE Internet Computing, 4(2).

Marsh, S. (1994). Formalising Trust as a Computational Concept. (Doctoral dissertation, University of Stirling, 1994).

Maurer, U. (1996). Modeling a public-key infrastructure. Proceedings of the European Symposium of Research on Computer Security, LNCS, vol. 1146, pp. 325–350.

McKnight, D. H., & Chervany, N. L. (2000, August). What is Trust? a conceptual analysis and an interdisciplinary model. Proceedings of the 2000 Americas Conference on Information Systems (AMCI2000). AIS, Long Beach, CA.

McKnight, D. H., Choudhury, V. & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: an integrative typology. Information Systems Research, 13(3), 334-359.

McKnight, D. H., & Chervany, N. L. (2003). The meanings of trust. UMN university report. Retrieved December 2006, from http://misrc.umn.edu/wpaper/WorkingPapers/9604.pdf

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of Management Review, 20(3), 709–734.

Miller, N. H., Resnick, P., & Zeckhauser, R. J. (2002). Eliciting honest feedback in electronic markets. KSG Working Paper Series RWP02-039.

Mui, L. (2003). Computational models of trust and reputation: agents, evolutionary games, and social networks. (Doctoral dissertation, Massachusetts Institute of Technology, 2003).

Pavlou, P. & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. Information Systems Research 15(1), 37–59.

Pennington, R., Wilcox, H. D. & Grover, V. (2004). The role of system trust in business-to-consumer transactions. Journal of Management Information Systems 20(3), 197–226.

Perlman, R. (1999). An overview of PKI trust models. IEEE Network, 13(6), 38–43.

Pujol, J. M., Sanguesa, R. & Delgado, J. (2002). Extracting reputation in multi-agent systems by means of social network topology. Proceedings of the First International Joint Conf. Autonomous Agents and Multiagent Systems.

Reiter, M. K., & Stubblebine, S. G. (1998). Resilient authentication using path independence. IEEE Transactions on Computer, 47(12), 1351–1362.

Resnick, P., & Zeckhauser, R. (2002, November). Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system. In M. Baye, Editor (Eds.) Advances in Applied Microeconomics: The Economics of the Internet and E-Commerce, 11, 127–157.

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

Rutter, J. (2001). From the sociology of trust towards a sociology of 'e-trust'. International Journal of New Product Development & Innovation Management 2(4), 371–385.

Sabater, J., & Sierra, C. (2002). Reputation and social network analysis in multi-agent systems. Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems.

Salam, A. F., Iyer, L., Palvia, P, & Singh, R. (2005). Trust in e-commerce. Communications of the ACM 48(2), 73–77.
Sarkio, K., & Holtmanns, S. (2007). Tailored trustworthiness estimations in peer to peer networks. To appear in International Journal of Internet Technology and Secured Transactions IJITST, Inderscience.
Sen, S., & Sajja, N. (2002). Robustness of reputation-based trust: boolean case. Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems.
Singh, A., & Liu, L. (2003). TrustMe: anonymous management of trust relationships in decentralized P2P systems. Proceedings of the IEEE International Conference on Peer-to-Peer Computing, pp. 142–149.
Song, S., Hwang, K., Zhou, R., & Kwok, Y. K. (2005). Trusted P2P transactions with fuzzy reputation aggregation. IEEE Internet Computing, 9(6), 24–34.
Sun, Y., Yu, W., Han, Z., & Liu, K. J. R. (2006). Information theoretic framework of trust modeling and evaluation for ad hoc networks. IEEE Journal on Selected Area in Communications, 24(2), 305–317.
Tan, Y. & Thoen, W. (1998). Toward a generic model of trust for electronic commerce, International Journal of Electronic Commerce, 5(2), 61–74.
TCG, Trusted Computing Group, Trusted Platform Module - TPM Specification v1.2, 2003. Retrieved May, 2006, from https://www.trustedcomputinggroup.org/specs/TPM/
Theodorakopoulos, G., & Baras, J.S. (2006). On trust models and trust evaluation metrics for ad hoc networks, IEEE Journal on Selected Areas in Communications, 24(2), 318–328.
Tajeddine, A., Kayssi, A., Chehab, A., & Artail, H. (2005, September). A comprehensive reputation-based trust model for distributed systems. Proceedings of the Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, pp. 118–127.
Wang, Y., & Varadharajan, V. (2005, July). Trust^2: developing trust in peer-to-peer environments**.** Proceedings of the IEEE International Conference on Services Computing, vol.1, pp. 24–31.
Guo, W., Xiong, Z., & Li, Z. (2005, September). Dynamic trust evaluation based routing model for ad hoc networks. Proceedings of International Conference on Wireless Communications, Networking and Mobile Computing, vol. 2, pp. 727–730.
Xiong, L., & Liu, L. (2004). PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities**,** IEEE Transactions on Knowledge and Data Engineering, 16(7), 843–857.
Yan, Z., & MacLaverty, R. (2006, September). Autonomic trust management in a component based software system. Proceedings of 3rd International Conference on Autonomic and Trusted Computing (ATC06), LNCS vol. 4158, pp. 279–292.
Yan, Z., & Prehofer, C. (2007). An adaptive trust control model for a trustworthy software component platform. Proceedings of the 4th International Conference on Autonomic and Trusted Computing (ATC2007), LNCS vol. 4610, pp. 226-238.
Yan, Z. (2006). A conceptual architecture of a trusted mobile environment. Proceedings of IEEE SecPerU06, France, pp. 75–81.
Yan, Z., Zhang, P., & Virtanen, T. (2003). Trust evaluation based security solution in ad hoc networks. Proceedings of the Seventh Nordic Workshop on Secure IT Systems (NordSec03), Norway.

Yu, B., & Singh, M.P. (2000). A social mechanism of reputation management in electronic communities. Proceedings of the Seventh International Conference on Cooperative Information Agents.

Zacharia, G., & Maes, P. (2000). Trust management through reputation mechanisms. Applied Artificial Intelligence, vol. 14, No. 8.

Zhou, M., Mei, H., & Zhang, L. (2005, September). A multi-property trust model for reconfiguring component software. Proceedings of the Fifth International Conference on Quality Software QAIC2005, pp. 142–149.

Zhang, Z., Wang, X., & Wang, Y. (2005, August). A P2P global trust model based on recommendation. Proceedings of the 2005 International Conference on Machine Learning and Cybernetics, vol. 7, pp. 3975–3980.