A Survey on Trust Modeling

JIN-HEE CHO and KEVIN CHAN, US Army Research Laboratory
SIBEL ADALI, Rensselaer Polytechnic Institute

28

The concept of trust and/or trust management has received considerable attention in engineering research communities as trust is perceived as the basis for decision making in many contexts and the motivation for maintaining long-term relationships based on cooperation and collaboration. Even if substantial research effort has been dedicated to addressing trust-based mechanisms or trust metrics (or computation) in diverse contexts, prior work has not clearly solved the issue of how to model and quantify trust with sufficient detail and context-based adequateness. The issue of trust quantification has become more complicated as we have the need to derive trust from complex, composite networks that may involve four distinct layers of communication protocols, information exchange, social interactions, and cognitive motivations. In addition, the diverse application domains require different aspects of trust for decision making such as emotional, logical, and relational trust. This survey aims to outline the foundations of trust models for applications in these contexts in terms of the concept of trust, trust assessment, trust constructs, trust scales, trust properties, trust formulation, and applications of trust. We discuss how different components of trust can be mapped to different layers of a complex, composite network; applicability of trust metrics and models; research challenges; and future work directions.

Categories and Subject Descriptors: H.1 [**Information Systems**]: Models and Principles

General Terms: Modeling, Human Factors, Algorithms, Networks

Additional Key Words and Phrases: Trust modeling, trust, trustor, trustee, decision making, composite trust

ACM Reference Format:
Jin-Hee Cho, Kevin Chan, and Sibel Adalı. 2015. A survey on trust modeling. ACM Comput. Surv. 48, 2, Article 28 (October 2015), 40 pages.
DOI: http://dx.doi.org/10.1145/2815595

1. INTRODUCTION

Trust has been broadly studied in many different disciplines and used as the basis for decision making in diverse contexts. Although different disciplines define trust differently, the problems they aim to solve have the common goals of accurate assessment of trust as a robust basis for decision making where inaccurate trust estimation can allow a trustor to place false trust in a trustee (i.e., mistrust), leading to a betrayal by the

Research was in part sponsored by the Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF-09-2-0053. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation here on. This research was also partially supported by the Department of Defense (DoD) through the Office of the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)). The views and opinions of the author(s) do not reflect those of the DoD nor ASD(R&E).
Authors' addresses: J.-H. Cho and K. S. Chan, 2800 Powder Mill Rd., Adelphi, MD 20783; emails: {jin-hee.cho.civ, kevin.s.chan.civ}@mail.mil; S. Adalı, Department of Computer Science, Rensselaer Polytechnic Institute, 110 8th Street, Troy, NY 12180; email: sibel@cs.rpi.edu.

DOI: http://dx.doi.org/10.1145/2815595

trustee or losing opportunities with good collaborators. In particular, as perfect knowledge is not available in many problem domains, the critical decisions are often made with uncertain, incomplete, and conflicting information. This uncertainty exposes the decision maker to risk of loss from incorrect decisions due to possible misplaced trust in another entity.

Yamamoto [1990] suggests that trust is a crucial component of social life. Individuals in societies continue to interact with each other as a direct result of their expectation of positive outcomes of such interactions [Yamamoto 1990]. These interactions result in relationships based on trust, in which individuals act in a way with the aim of maintaining future positive interactions, instead of acting out of self-interest [Gambetta 1988]. That is, after cooperative behavior to maximize self-interest (i.e., utility) results in a trust relationship between two entities, it can also enhance their cooperation, leading to a virtuous cycle of mutual benefit based on the trust relationship.

Past surveys on trust research are often limited to a particular research domain, such as trust metrics in data fusion [Blasch et al. 2014], trust management in mobile ad hoc networks (MANETs) [Cho et al. 2011], and trust and reputation systems in online services [Jøsang et al. 2007]. Different from the prior work, this survey brings together the core aspects of trust modeling from different domains. In addition, we introduce the concept of *composite trust,* which can be derived from the mixture and/or interplay of the trust characteristics from different domains. We pose the problem of trust modeling in a complex, composite network setting to build multilayered trust dimensions as follows:

—Communication trust from communication networks such as quality of service (e.g., service response time, packet drop rates)
—Information trust from information networks (e.g., information credibility, veracity, integrity)
—Social trust from interactions/networks (e.g., a source's reliability)
—Cognitive trust from cognitive process (e.g., cognitive information processing capability)

For example, when Alice receives information from Bob, they often use communication media (e.g., email, phone, text, social network services or media). Depending on the quality of service (QoS) received by the interacting entity, Alice's trust toward the information and/or source of the information may be adjusted, such as high delay of a message delivered. In addition, the received information can be analyzed based on many different criteria to capture quality of information (QoI) that may include correctness, completeness, credibility, and/or relevance. If Alice knows Bob in her social network, Alice can also infer the trust of the information based on Bob's reputation (e.g., influence, centrality), social ties, and/or similarity in the social network. When Alice needs to make a certain decision based on Bob's advice, how to filter Bob's advice on Alice's side is also dependent upon Alice's cognitive constructs such as tendency, competence, and/or feeling as well as other situational factors such as risk and uncertainty inherent in the decision.

This article aims to give a good starting point for trust researchers by providing efficient and relevant background knowledge on how to model trust in a given domain. This article deals with the following topics:

—What is trust? How has trust been defined in different disciplines? What are the key factors that affect trust assessment of an entity? (Section 2)
—How is trust measured in the continuum from distrust to trust? How does one put trust on a scale (e.g., binary, discrete, continuous)? (Section 3)

Table I. Multidisciplinary Definitions of Trust

Discipline	Meaning of Trust	Source
Sociology	Subjective probability that another party will perform an action that will not hurt my interest under uncertainty and ignorance	Gambetta [1988]
Philosophy	Risky action deriving from personal, moral relationships between two entities	Lahno [1999]
Economics	Expectation upon a risky action under uncertainty and ignorance based on the calculated incentives for the action	James [2002]
Psychology	Cognitive learning process obtained from social experiences based on the consequences of trusting behaviors	Rotter [1980]
Organizational Management	Willingness to take risk and being vulnerable to the relationship based on ability, integrity, and benevolence	Mayer et al. [1995]
International Relations	Belief that the other party is trustworthy with the willingness to reciprocate cooperation	Kydd [2005]
Automation	Attitude that one agent will achieve another agent's goal in a situation where imperfect knowledge is given with uncertainty and vulnerability	Lee et al. [2006]
Computing & Networking	Estimated subjective probability that an entity exhibits reliable behavior for particular operation(s) under a situation with potential risks	Cho et al. [2011]

—What are the constructs of trust? How can they be formulated in a certain dimension? What constructs can be mapped to measure the so-called composite trust derived from a complex, composite network? (Section 4)
—What are the properties of trust and how are they modeled? (Section 5)
—What are the applications of trust in computing and engineering fields? What are the challenges and suggestions in modeling trust? (Section 6)
—Concluding remarks (Section 7)

2. CONCEPT AND ANALYSIS OF TRUST

2.1. Multidisciplinary Definitions of Trust

The dictionary definition of trust is "assured reliance on the character, ability, strength, or truth of someone or something" [Merriam and Webster Dictionary 2015]. In essence, trust is a relationship in which an entity, often called the trustor, relies on someone or something, called the trustee, based on a given criterion. As trust is a multidisciplinary concept, the term has been used in different disciplines to model different types of relationships: trust between individuals in social or e-commerce settings, trust between a person and an intelligent agent in automation, and trust between systems in communication networks [Cho et al. 2011]. Before we give a common definition of trust that encompasses these concepts, we briefly survey the definitions of trust in different fields and across disciplines. We then use these definitions to arrive at a multidisciplinary definition of trust.

Social sciences often study trust between individuals in social settings. However, some definitions of trust look at trust in other entities like organizations and countries. In social settings, individuals have expectations of behavior from each other. In a classical definition from *Sociology*, Gambetta [1988] defines trust as the trustor's subjective probability about whether the trustee (or trustees) will perform a particular action that benefits the trustor. The probability is assessed before the trustee takes an action and in conditions of uncertainty regarding the trustee. In this model, trust exists if the probability exceeds a threshold. He clarifies the relationship between trust and cooperation in that trust is one possible result of cooperation, not the precondition

of cooperation. Agents can cooperate due to self-interest or obligation, not trust. If two agents trust each other, they would be more willing to cooperate.

Despite the modeling of trust as a subjective probability, it is often treated as the trustor's belief about the trustee. A great deal of research concentrates on the nature of this belief from the perspective of the trustor.

In *Philosophy*, for example, trust is a personal, internal phenomenon that helps maintain moral relationships between individuals. In particular, according to Lahno [1999], betrayal of trust is a clear violation of moral behavior, leading to distrust.

In *Economics*, trust is commonly studied from the perspective of a trustor's motivations for cooperation in risky situations. The source of the risk is that the trustee may choose not to cooperate and cause a loss of utility for the trustor. The trustor's decision to trust an individual is based on a rational decision to maximize its own interest by choosing the best compromise between risk and possible utility from cooperation. This model of trust has been debated by psychologists and behavioral economists who have shown many examples of irrational behavior by individuals in the strict utility sense.

In *Psychology*, Rotter [1980] describes trust as a cognitive construct an individual learns from social experience such as positive or negative consequences of trusting behavior. He concludes that if a person has had negative experiences by trusting more in the past, the person is not likely to trust in the future, or vice versa. Propensity to trust is a well-accepted construct, showing differences in the level of trust between individuals in the same situation.

It is clear from these studies that a human trustor's individual characteristics, motivation, and social and cultural background will impact how much he or she will trust another agent. However, even individuals with the same propensity to trust will differ in their trust levels depending on the given situation. In particular, trust beliefs are highly impacted by who or what the trustee is. Other work concentrates on modeling the trustworthiness of the trustee.

In *International Relations*, Kydd [2005] describes trust as the belief that the other party is trustworthy with the willingness to reciprocate cooperation. On the other hand, mistrust is to believe that the other party is untrustworthy in order to exploit one's cooperation. Trust and mistrust between nations have been discussed as important issues because they can lead to peace or war.

In *Organizational Management*, Mayer et al. [1995] define trust as the willingness of the trustor to take risk and be vulnerable based on the ability, integrity, and benevolence of the trustee. The definition of trust based on these three dimensions of the trustee has been extensively used in different areas, especially in fields like automation and other fields of computing and engineering in modeling trust of a human toward a machine's automated operations.

In different computing fields, various definitions of trust exist. When the trustor is a computational agent, the individual characteristics of the trustor are not relevant to the model. In these cases, models concentrate on understanding the trustworthiness of the trustee based on past behavior.

In *Automation*, Lee and See [2006] see trust as the attitude that one agent will achieve another agent's goal in a situation where imperfect knowledge is given with uncertainty and vulnerability. The trustee is often an automation system, while the trustor can be either a person or another computational agent. The main goal in automation, called trust calibration, is to assess whether the trustor's trust beliefs reflect the actual ability of the automation to achieve a task. The reliability aspect of the trust belief models whether the system is operating within design parameters or not.

In *Computing and Networking*, the concept of trust is used in many different fields ranging from artificial intelligence to human–machine interaction to networking (e.g., telecommunication, social network analysis, communication networks, and

cyber/network security) [Cho et al. 2011; Adalı 2013]. An agent's trust is a subjective belief about whether another entity will exhibit behavior reliably in a particular context with potential risks. The agent can make a decision based on learning from past experience to maximize its interest (or utility) and/or minimize risk [Cho et al. 2011; Li et al. 2008].

Across disciplines, we summarize the concept of trust based on the common themes as follows.

Trust is the willingness of the trustor (evaluator) to take risk based on a subjective belief that a trustee (evaluatee) will exhibit reliable behavior to maximize the trustor's interest under uncertainty (e.g., ambiguity due to conflicting evidence and/or ignorance caused by complete lack of evidence) of a given situation based on the cognitive assessment of past experience with the trustee.

2.2. Analysis of Trust Assessment

Based on the previous discussion on the multidimensional concept of trust, we incorporate various concepts of trust to describe how an entity assesses another entity's trust and how the trust evolves over time. Figure 1 explains each term and step used to describe how "Trustor i assesses Trustee j's trust if j can perform Task A." Here we discuss them in detail as follows.

Trustor i is a cognitive entity that has the learning ability to estimate trust of a trustee to maximize its interest (or utility) from the relationship with the trustee. Game-theoretic approaches have been used to model utility functions of an agent in various domains [Chin 2009].

Trustee j is an entity that can cause some impact on a trustor's interest by the outcome of its behavior [Castelfranchi and Falcone 2010].

Trust Assessment is the process that trustor i employs to assess trust for trustee j, incorporating different considerations on both individual and relational levels from the mood of the trustor to the reliability of the trustee as well as the influence of the trustee in a social network. We discuss these diverse considerations in Section 4 and summarize them in Figure 1.

Risk Assessment is a critical phase for objective assessment of trust. This can be conducted based on three dimensions: uncertainty/ambiguity, vulnerability, and impact. Uncertainty comes from lack of evidence to estimate trust, while ambiguity derives from conflicts of evidence from multiple sources toward a same proposition. The amount of relevant evidence can lead i to make a decision on whether to trust j. Vulnerability is how easily trustee j can betray and exploit i's trust in j in order to pursue j's goal that may hurt i's interest. Impact is the measure of consequence when i's decision fails by either being betrayed by j or losing opportunities to achieve i's goal.

Importance of Task A **to Trustor** i is also a significant factor for i to decide whether to trust j. If j behaves as i expects and trusting j gives higher benefit to i than not trusting j, i is more likely to take risk in trusting j. According to Gambetta [1988], cooperation is not the result of trust, while trust is the result of the cooperation-based mutual benefit of helping each other. However, the mutual trust generated by the initial cooperation can enhance continuous cooperation in repeated games. We discuss *cooperation* in detail as a factor that affects trust relationships in Section 2.3.

Through the risk assessment and the importance of A, i can estimate the utility of either decision and can choose one that gives a higher utility. Note that the utility is computed based on the gain and loss of each decision. When the utilities of the two decisions are equal, then i keeps searching for more evidence to make a decision.

Outcome is the result after the decision is made. Depending on whether the decision turns out to be right or wrong, trust is adjusted accordingly. This is called

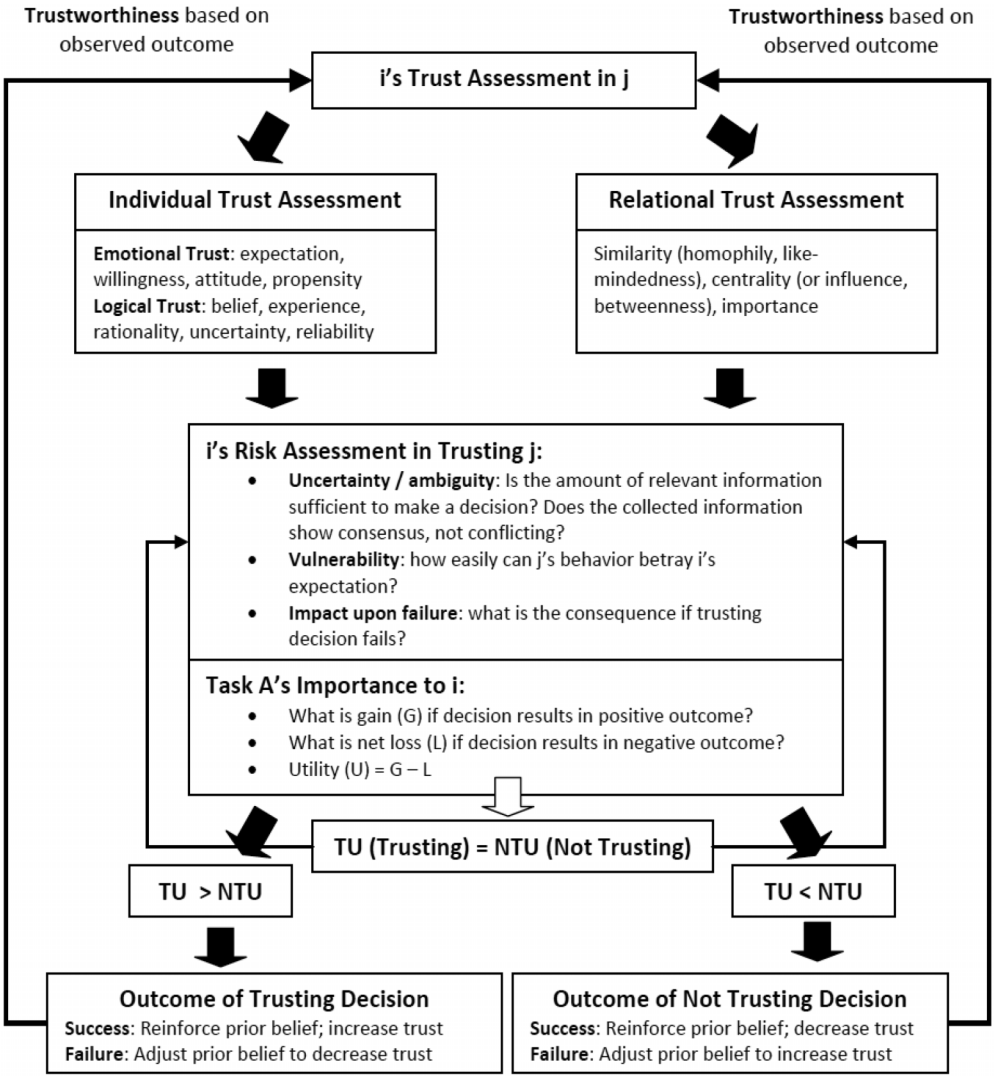


Fig. 1. Analysis of the trust assessment process.

trustworthiness, which represents objective trust based on observed outcome, while overall trust can be formed based on the combination of subjective trust and objective trust. The trustworthiness is the trust validated through the actual evidence. The outcome is fed back to the trust assessment cycle in repeated situations. That is, validated trust can reinforce the prior belief, while betrayed trust can fix the prior belief and update the current belief based on the new evidence. In this sense, the mental process of trust assessment is *recursive* in nature because a prior belief generates an outcome that is fed back as the input to update trust.

Romano's classification on the concept of trust [2003] is well aligned with the process of trust assessment described in Figure 1. Romano [2003] categorizes the concept of trust in terms of *phenomenon*, *sentiment*, and *judgment*. These three criteria match the stages of trust assessment. First, *phenomenon-based* trust explains how a trustor

forms trust in a trustee based on the perceived social and functional phenomenon (e.g., observed behavior) by his or her subjective attitude. Second, *sentiment-based* trust addresses utility analysis related to why the trustor needs to trust a trustee or not. This explains how the trustor is motivated to trust the trustee, what would be a consequence if the decision fails, and what the degree of calibrated risk is associated with uncertainty. This state is in line with risk assessment and a task's importance associated with a trustor's interest explained in Figure 1. Lastly, *judgment-based* trust is associated with how trust is measured and updated. This is well matched with the state of reinforcing and updating prior belief based on the outcome of the prior decision, which is new evidence in a cycle of trust assessment.

2.3. Factors Affecting Trust

How an entity assesses another entity's trust can be affected by other conditions, which include internal and/or external properties such as an individual's psychological states and social/political relationships of the two entities. Now we look at concepts that can be observed in relationships between entities and how they can affect trust relationships.

Risk critically affects trust relationships. Trust is the willingness to take risk under uncertainty [Luhmann 1979]. Risk may be estimated based on the degree of harm multiplied by its likelihood. Castelfranchi and Falcone [2010] distinguish objective risk from subjective risk. Objective risk is perceived by external ideal observer(s), while subjective risk is perceived by an individual entity. Luhmann [1979] defines risk differently from a danger. The danger may exist regardless of the decisions made by an entity, while risk is triggered based on the decision made by the entity. Deciding to use trust for decision making implies that a trustor is willing to accept risk [Luhmann 1979; Boon and Holmes 1991]. Jøsang and Presti [2004] and Solhaug et al. [2007] discuss that trust is not necessarily proportional to the reverse of risk because risk may exist even under a situation with high trust. By applying the relationship between trust and risk, the balance between trust and risk can be investigated for optimizing gains by trust decisions.

Faith is a belief based on nonrational grounds [Castelfranchi and Falcone 2010]. Strict faith does not allow doubt by searching evidence and goes against counterevidence. If trust is evidence based, faith is contrary to trust. However, faith may be triggered by evidence, signs, or experience. But even if faith may be triggered by some evidence, after it is formed, it is less likely to be changed.

Fear is "perceived risk" that is unbearable or unmanageable [Lazarus et al. 1970]. Fear represents extreme lack of trust as part of distrust and can increase if a trustor is exposed or unprotected by the consequence of the failure of its trust relationship.

Feeling is something that entity i "feels" about entity j like confidence, not judgment [Castelfranchi 2009]. *Feeling-based trust*, in contrast to *reason-based trust* (e.g., evidence-based evaluation), can be formed based on explicit experiences, dispositions, intuition, knowledge, and/or implicit learning.

Valence implies a positive or negative as the key factor affecting trust. Dunn and Schweitzer [2005] show that positive valence (e.g., happiness, hope) increases trust, while negative valence (e.g., fear, guilty) decreases trust.

Faith, fear, feeling, and valance are the components related to an individual's difference in terms of a perspective to perceive things and/or situations that affect trust assessment. Accordingly, they significantly affect decision making even without any evidence.

Power given unequally between two entities can put their trust relationship in danger [Farrell 2009] because trust cannot be maintained in a situation of extreme disparities of power. But trust may exist in relationships where disparities of power between two entities exist but are less pronounced. Farrell distinguishes when power

over one entity is derived out of trust from when power and trust are not mutually exclusive (e.g., complying to a given authority, not because of trusting).

Delegation occurs when an entity wants to exploit the actions of other entities for achieving its goal. The formal definition can be "entity i delegates entity j to perform action α for achieving goal φ" [Castelfranchi 2009]. The trust of entity i in entity j is not the precondition of delegation of task φ to entity j. *Dependence-based delegation* occurs when action α of entity j is a necessary condition to achieve goal φ regardless of the fact that entity i trusts entity j. On the other hand, *preference-based delegation* means that entity i believes that goal φ can be more likely to be achieved by action α based on entity i's preference [Castelfranchi 2009]. Norman and Reed [2010] discuss how responsibility can be transferred in the process of delegation.

Control is an action that aims at (1) ensuring successful achievement of a certain task by monitoring (or providing feedback) and (2) intervening in the middle of performing a task not to degrade performance [Castelfranchi and Falcone 2000]. Control often kills trust such that entity i tries to control entity j because entity i does not trust entity j. However, when control is properly used, it can be complementary to trust, resulting in increased trust between two entities while mitigating risk.

Credit can be given from uncertainty in a situation where a trust decision should be made, depending on a trustor's attitude or prior trust toward a trustee. Trust is more than a belief based on evidence that gives a certain level of confidence. In particular, when uncertainty exists, trust can give "credit" for the uncertainty. For example, when 50% of trust can be explained based on evidence, it does not mean the other 50% shows distrust, but it would just represent lack of evidence, which can be given as credit [Castelfranchi and Falcone 2000; Jøsang et al. 2006].

Cooperation has been thought of as the result of trust relationships between entities. However, some researchers discuss that the foundation of cooperation is not trust but the durability of the relationship based on possibilities for mutual rewards [Gambetta 1988]. Axelrod [1981] explains that cooperation emerges given an indefinite number of interactions. An individual entity cannot prosper without being cooperative with other entities. Depending on context, there may be a situation in which trust does not play a key role in triggering cooperation. However, as cooperative interactions evolve, trust can emerge and be fed back to trigger other cooperative behavior for reciprocation.

Altruism refers to an act that benefits another entity, which is not closely related (e.g., not relatives), while being obviously harmful to the entity performing the altruistic behavior [Trivers 1971]. Trivers [1971] formalizes an altruistic act as the higher net benefit given to a recipient than one to a performer of the act. In this sense, trust is explained as one of the factors to regulate the altruistic system where trust-induced reciprocation can circulate or foster altruistic behavior or vice versa.

Reciprocation is commonly observed in societies of animals or insects such as bats [Harcourt 1991], chimpanzees, and cetaceans [Trivers 1985]. If one acts in favor of another, the favor is expected to be returned now or some time later. Reciprocation tends to benefit the reciprocator in the long run. Reciprocators will be more likely to have the benefits of their cooperative behaviors to others, distinguished from cooperative behaviors based on purely altruistic motives. Reciprocation contributes to reasoning trust. Computing the net benefit of reciprocation may need to consider aspects of memory in terms of the time for the reciprocation to be returned.

Adoption is an action to accept or choose something or someone to achieve a certain goal. According to Hardin [2002], a self-interested (i.e., "self-driven" and "self-motivated," but distinguished from being "selfish") agent can adopt another entity's goal to achieve its goal. For example, if we order to ship an item online by paying money, we trust the item will arrive within several days. That is, the trustee acts as

the trustor expected but the trustee acts that way for his or her own benefit. However, the trustor's decision to adopt the trustee's goal is based on its trust in the trustee [Falcone and Castelfranchi 2001].

Social or Relational Capital can be viewed as trust of an individual as a strategic resource, such as how to be selected from other potential partners to establish cooperation / collaboration via accumulated trust [Castelfranchi and Falcone 1998a]. Most trust research examines trust evaluation in terms of a trustor's perspective, such as how to select the right collaborators to complete his or her goals. Burt [2000] and Coleman [1988] view *social capital* as the benefits that individuals or groups have because of their location (or status) in social structure. Bourdieu [1983] explains that social capital is obtained through all possible resources from relationships in social networks an entity (person) is associated with. Putnam [2000] indicates that social capital can be trust, norms, and networks of a social organization. *Relational capital* is a capital for individuals. As the perspective of a trustee, relational capital is the basis of the social capital that can give social power in a network [Castelfranchi and Falcone 1998b].

Norms, Regulations, Laws, and Contract are often placed for a trustor to be protected from possible risk when there is no trust between the parties [Castelfranchi 1995]. Some types of regularity and normality are introduced for a trustor to be protected when a trustee violates the contract. However, the key issue is not trust between two parties, but how to enforce the contract [Castelfranchi 1995]. Trust is needed to achieve the goal for the two parties to make a contract. However, there should be more trust of the trustee in the authority that enforces the contract, which may generate fear upon breaking the contract and lead the trustee to follow the contract. A different type of trust, called *institutional trust*, is needed in this context [Castelfranchi 1995].

The terminologies discussed here can be examined in terms of how they affect the relationships between two entities and how trust is affected by their dynamics. Table II summarizes the definitions of the these concepts [Merriam and Webster Dictionary 2015] and correspondingly their relationships with trust based on our discussion in this section.

3. MEASUREMENT OF TRUST

3.1. Continuum of Trust

Different levels of assessed trust are often called by different terms representing low trust, misdiagnosed trust, or a mixture of the two. In this section, we give clear distinctions of the concept of trust from other associated concepts including distrust, untrust, undistrust, mistrust, and misdistrust. In addition, we demonstrate the continuum of trust in which each term can be used to indicate a certain range of the trust continuum. Now we start to look into what each term means and how it is formulated in the literature.

Trust is a belief that does not necessarily require observed behavior in the past, that is distinct from trustworthiness, which is a verified objective of trust through observed evidence [Solhaug et al. 2007]. Thus, trust includes both subjective and objective trust (i.e., trustworthiness). Trust can be simply notated as [Marsh 1994].

$$T(i, j, \alpha). \tag{1}$$

This notation reads as "i trusts j in a situation α." Marsh [1994] defines trust as a real number scaled in $[-1, 1]$, where 0 indicates complete uncertainty or ignorance.

Specifying the aspects of motivational actions of trusting behavior in a situation, Castelfranchi [2009] defines general trust, called the *core trust*, by

$$CoreTrust(i, j, \varphi) \doteq \bigvee_{\alpha \in A} CoreTrust(i, j, \alpha, \varphi). \tag{2}$$

Table II. Concepts Affecting Trust Relationships

Concept	Definition	Relationship with Trust
Risk	Possibility that something bad or unpleasant (such as an injury or a loss) will happen	Trust is the degree of willingness to take risk
Faith	Strong belief or trust in someone or something	Faith can be triggered by trust and is less likely to be changed when it is formed
Fear	Being afraid or worried of something or someone	Fear represents the extreme lack of trust
Feeling	An emotional state or reaction	Feeling affects forming trust based on individuals' characteristics in knowledge, experiences, intuition, and dispositions
Valence	Degree of attractiveness an individual, activity, or thing possesses as a behavioral goal	Positive valence increases trust, and vice versa
Power	Ability or right to control people or things	Unequal power relationships can endanger trust
Delegation	Act of giving control, authority, a job, or a duty to another person	Trust may trigger delegation based on preference
Control	Directing the behavior of (a person or animal); causing (a person or animal) to do what you want	Control may kill trust; but when it is properly used, it can be complementary to trust in mitigating risk
Credit	Provision of money, goods, or services with the expectation of future payment	Trust can give credit for uncertainty derived from lack of evidence
Cooperation	A situation in which people work together to do something; the actions of someone who is being helpful by doing what is wanted or asked for	Repeated cooperative interactions may trigger trust, which can be fed back to cooperative behaviors
Altruism	Unselfish regard for or devotion to the welfare of others	Trust can regulate and foster altruistic behavior
Reciprocation	A mutual exchange	Reciprocation contributes to reasoning trust, which fosters cooperative behaviors
Adoption	Act or process of giving official acceptance or approval to something	A trustor's decision to adopt a trustee lies in his or her trust in the trustor
Social Capital	Benefits that individuals or groups have because of their location (or status) in social structure	Trust relationships are the capital to gain social power
Relational Capital	A capital that can gain from all relationships in an individual	Trust relationships are the capital to gain relational power
Contract	A legal agreement or document between people, companies, etc.	A contract based on norms, regulations, or laws is placed to protect trust relationships from possible risk due to lack of trust

Here, entity i trusts entity j to achieve goal φ by action α if and only if there exists some action α where A is the set of actions through which entity i can act toward entity j.

Compared to the Marsh [1994] definition of trust in Equation (1), the *core trust* is a generalized formulation of trust by specifying internal properties (i.e., goal φ) and external properties (i.e., actions αs) of a trustor i that can act toward a trustee j.

Distrust is not simply the complement of trust [Pereitra 2009]. Trust and distrust may not be derived from the same information but can coexist without being complementary [Marsh and Dibben 2005; Luhmann 1990; Pereitra 2009]. For example, i may not trust j due to lack of information, but this does not mean i distrusts j [Pereitra 2009]. When i believes that j has negative intentions toward i, this is distrust. Marsh

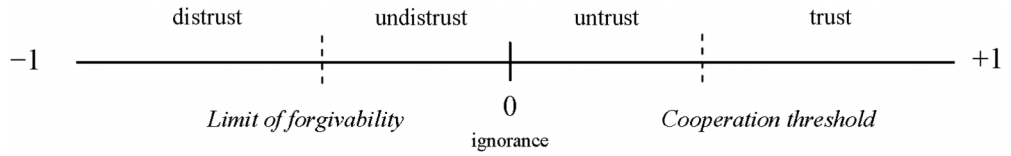


Fig. 2. Trust continuum: trust, untrust, undistrust, and distrust.

and Briggs [2009] formulate distrust by

$$T(i, j, \alpha) < 0 \Longrightarrow Distrust(i, j, \alpha). \tag{3}$$

$T(i, j, \alpha) < 0$ indicates that trust is below the ignorance value 0, where the higher the value is, the higher the trust that exists between i and j in situation α. The previous equation reads as "i believes that j will be actively against i's best interest in situation α." Castelfranchi [2009] also defines distrust by

$$Distrust(i, j, \varphi) \doteq \bigvee_{\alpha \in A} Distrust(i, j, \alpha, \varphi). \tag{4}$$

Similar to the core trust defined in Equation (2), this distrust formulation provides internal and external properties of a trustor i that can act toward a trustee j. The previous equation reads as entity i distrusts entity j to ensure goal φ by doing all actions αs.

Untrust is defined as the state in which a trustee cannot reach the cooperation threshold in terms of its capability. For example, i does not distrust j, but i cannot trust j since j does not have the capability to perform task α or i does not have sufficient evidence to trust j [Marsh and Briggs 2009]. Untrust can be represented as

$$T(i, j, \alpha) > 0 \ \wedge \ T(i, j, \alpha) < Th^{cooperation}(i, j, \alpha) \ \Longrightarrow Untrust(i, j, \alpha). \tag{5}$$

Cofta [2007] calls this concept of untrust "mixed trust." Different from untrust or distrust, usually ignorance or ambivalence indicates $T(i, j, \alpha) = 0$.

Undistrust means the lack of trust [Griffiths 2006] indicating when a trustor cannot sufficiently make a decision for whether he or she distrusts a trustee. Castelfranchi [2009] defines a similar concept, called "lack of trust," as

$$LackTrust(i, j, \varphi) \Longrightarrow \bigvee_{\alpha \in A} LackTrust(i, j, \alpha, \varphi). \tag{6}$$

This means that "entity i lacks in trust in entity j to ensure goal φ by performing all actions αs." Although the lack of trust does not necessarily mean distrust, distrust may mean lack of trust. Marsh and Briggs [2009] introduce a threshold to distinguish undistrust from distrust using the concept of forgiveness. We similarly formulate the limit of forgiveness as the distrust threshold by

$$Th^{forgiveness}(i, j, \alpha) < T(i, j, \alpha) < 0 \Longrightarrow Undistrust(i, j, \alpha). \tag{7}$$

Marsh and Briggs [2009] demonstrate the continuum of trust, untrust, undistrust, and distrust. Figure 2 shows the thresholds distinguishing undistrust from distrust and untrust from trust with a "limit of forgivability" and "cooperation threshold," respectively [Marsh and Briggs 2009].

The concept of forgiveness is introduced through the mechanisms of redemption, recovery, or repairing in a system because selfish or malicious entities exhibit desirable behavior over time to regain their reputation or trust in order not to be isolated from a network [Cho et al. 2009; Wang and Wu 2007].

Table III. Distinctions of Trust, Distrust, Untrust, Undistrust, Mistrust, and Misdistrust

Trustor's Belief in a Trustee	Trust	Distrust	Untrust	Undistrust	Mistrust	Misdistrust
Capability to perform task X	Yes	Yes/No	No	Yes/No	Yes	No
Negative intention	No	Yes	No	Yes/No	No	Yes
Cooperation threshold	Above	Below	Below	Below	Above	Below
Forgivability threshold	Above	Below	Below	Above	Above	Below

Mistrust derives from misinformation, often called *misplaced trust*, where a trustee does not have the intention to betray a trustor [Marsh and Briggs 2009]. Castelfranchi [Castelfranchi 2009] defines "mistrust" by

$$Mistrust(i, j, \varphi) \Longrightarrow \bigvee_{\alpha \in A} Mistrust(i, j, \alpha, \varphi). \tag{8}$$

This means that "entity i mistrusts entity j to ensure $\neg\varphi$ (φ is not going to happen) by performing α." Mistrust implies distrust, but not vice versa. Type I error refers to false negatives, implying mistrust in the previous equation.

Misdistrust is defined as distrusting or ignoring an entity (or information) that is trustworthy [McGuinness and Leggatt 2006]. This is often categorized as Type II error, such as false positives in detection/observation. A trustor mistakenly diagnoses a trustee as untrustworthy.

Table III summarizes the previous five concepts and their unique characteristics based on the belief of a trustor in a trustee. In particular, mistrust and misdistrust are related to the accuracy of trust assessment or estimation where they mean misplacing trust or distrust on a trustee where the ground truth is the opposite, trusting for a distrusted entity and distrusting for a trusted entity.

The decision for whether an entity is trusted or not is often treated as a binary decision. When trust is evaluated in either discrete or continuous scale with different ranges of lower and upper bounds, the binary decision of trust can be made by using the trust threshold that can determine the trustworthiness of an entity, which is similar to the threshold of cooperation shown in Figure 2. Now we discuss how trust is measured in different scales in the literature.

3.2. Scaling Trust

The concept of trust is subjective in nature. Although many researchers have proposed different methods of scaling trust, there has been no standard of scaling trust so far. In this section, we survey how trust is measured with a different scaling manner in the literature and discuss how they can be explained on the continuum of trust and distrust.

Different scales of trust include binary, discrete, nominal scale, and continuous values. Table III gives the scales of trust measures found in the literature [Marsh 1994]. Noticeably, a binary scale to indicate trust level loses resolution, but it is simple and efficient to determine whether an entity is trusted or not. Dealing with trust as a number (either discrete or continuous) gives more flexibility for normalization or spotting outliers. Binary fashion of trust decision can be expanded to a situation in which an entity is treated as trusted when it has the trust level above a certain threshold, similar to the cooperation threshold shown in Figure 2. The trust threshold can be application dependent and can filter untrusted or distrusted entities out of a system based on system requirements.

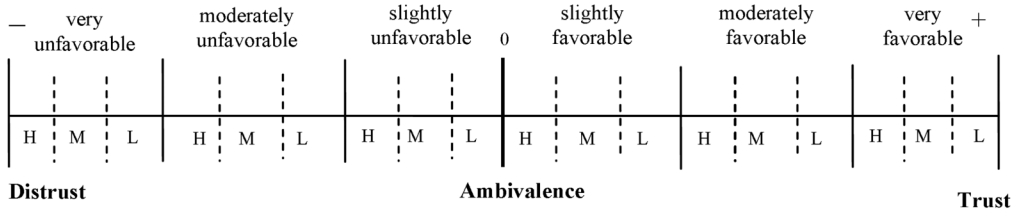
An entity uses different scales in evaluating its trust based on their judgments. The entity can have a favorable (positive) or unfavorable (negative) attitude toward another entity, taking a symmetric direction from complete trust to complete distrust.

Table IV. Various Scales of Trust Measurement

Normal	CD	VHD	HD	HMD	LMD	LD	LT	LMT	HMT	HT	VHT	CT
Binary	0						1					
Discrete	−6	−5	−4	−3	−2	−1	1	2	3	4	5	6
Continuous	−1					0						1

Ignorance

CD	Complete Distrust	CT	Complete Trust
VHD	Very High Distrust	VHT	Very High Trust
HD	High Distrust	HT	High Trust
HMD	High Medium Distrust	HMT	High Medium Trust
LMD	Low Medium Distrust	LMT	Low Medium Trust
LD	Low Distrust	LT	Low Trust



(Strength: H: High; M: Moderate; L: Low)

Fig. 3. Scaling trust and distrust on the continuum [Romano 2003].

When the entity decides the direction of trust, it can estimate the incremental degree of trust in the range of *slightly - moderately - very*. After that, the entity may have the perception to ensure the strength of trust, *high - moderate - low*. Figure 3 describes the continuum of trust and distrust. This is commonly used as an indicator of confidence in the literature. Now let us look into how various constructs of trust have been formulated in the existing work.

4. CONSTRUCTS OF TRUST

As trust is subjective in nature and context dependent, various dimensions of trust have been considered in different contexts with different purposes. Although other classifications may be possible, we view the concept of trust that can derive from individual and relational characteristics. Hence, we classify trust in two attributes: individual trust versus relational trust.

Individual trust attributes involve any trust dimensions that can be mainly derived from an individual's own characteristics. *Relational trust* attributes refer to the dimensions of trust that can emerge from the relationships with other entities (e.g., by comparing itself to others). The individual trust attributes can be classified in a twofold manner: logical trust and emotional trust. *Logical trust* indicates reasoning trust based on a logical cognition process of evidence or observations by an entity. On the other hand, *emotional trust* involves a reasoning process of trust using an individual's emotional sense such as feeling and propensity. Figure 4 summarizes the classification of constructs of trust in terms of individual and relational trust. And then individual trust has two aspects of attributes, such as logical trust and emotional trust. We discuss each construct of trust following the structure of the concepts demonstrated in Figure 4.

Based on our discussions of trust attributes in Sections 4.1 and 4.2, we will discuss how each trust attribute can be found in a different layer of a complex, composite

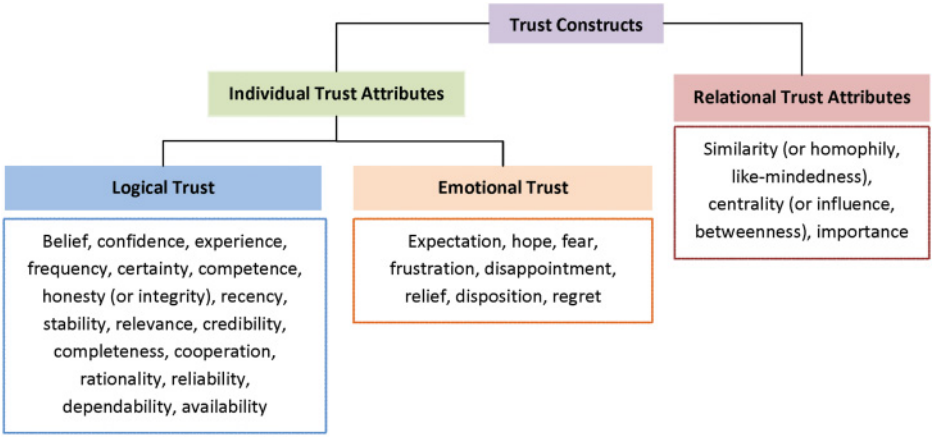


Fig. 4. Classification of factors affecting trust.

network in Section 4.3 and propose the concept of composite trust consisting of communication trust, information trust, social trust, and cognitive trust.

4.1. Individual Trust Attributes

4.1.1. Logical Trust. In this section, we discuss the components impacting trust of an entity that can be logically derivable based on observations or evidence.

Belief has been used as the root to estimate trust toward an entity for decision making. Many belief theories have been proposed since the 1970s, including Bayesian Inference [Fienberg 2006], Dempster-Shafer Theory [Shafer 1976], Transferrable Belief Model [Smets and Kennes 1994], Fuzzy Logic [Zadeh 1965], Subjective Logic [Jøsang 1999, 2001], and Dezert-Smarandache Theory (DSmT) [Dezert and Smarandache 2004]. Since each theory is very well known and contains a large volume of contents, interested readers can refer to Shafer [1976], Smets and Kennes [1994], Zadeh [1965], Jøsang [1999, 2001], and Dezert and Smarandache [2004] for details. Here we discuss how each theory has been used to propose trust models or schemes in computing and engineering domains.

Bayesian inference has been a popular technique to estimate trust [Zouridaki et al. 2005], where the beta distribution [Gillies 2000] is commonly applied. Given binary evidence such as "positive evidence a" and "negative evidence b" where a random variable r is in $[0, 1]$ and a, b is larger than 1, the pdf of the beta distribution follows

$$beta(r; a, b) = \frac{r^{a-1}(1-r)^{b-1}}{\int_0^1 r^{a-1}(1-r)^{b-1}dr}, \quad \text{where } 0 \le r \le 1. \tag{9}$$

Trust value as the mean of $beta(a, b)$ can be simply estimated as $a/(a + b)$.

Fuzzy logic has been used to manage uncertainty [Zadeh 1983] and to model trust in various network environments such as semantic web [Nagy et al. 2008; Lesani and Bagheri 2006], P2P [Chen et al. 2009], grid computing [Liao et al. 2009], mobile ad hoc networks [Luo et al. 2008], and e-commerce [Manchala 1998; Nefti et al. 2005].

Based on DST, Jøsang [1999, 2001] proposes the concept of *subjective logic* that describes subjectivity of an opinion (trust) in terms of uncertainty (u), belief (b), and disbelief (d), where $b + d + u = 1$. Subjective logic has been considerably used for developing various applications by many researchers. Lioma et al. [2010] use subjective logic to measure uncertainty in information fusion. Manna et al. [2010] extend subjective logic

to extract opinions from documents. Oren et al. [2007] propose a subjective-logic-based argumentation framework for evidential reasoning of a sensor to maximize its utility.

As an extension of DST, DSmT [Dezert and Smarandache 2004] has been proposed to deal with conflicting evidence that has not been properly handled by DST. DSmT has been applied in trust management for mobile ad hoc networks [Wang and Wu 2007] and trust-based service discovery mechanisms [Deepa and Swamynathan 2014].

Confidence is important to prove that an entity has sufficient experience to assess a particular trust dimension d [Griffiths 2006]. Griffiths [2006] proposes an interaction-based confidence computation in a particular trust dimension d and formulates it as

$$Confidence_i^d = I_i^{d+} + I_i^{d-}. \tag{10}$$

A trust dimension d can be replaced with another entity j in which the entity i evaluates another entity j. I_i^{d+} is the number of interactions with positive experience, and and I_i^{d-} is the number of interactions with negative experience. Griffiths [2006] uses the previous confidence calculation in order to determine to which the trust of an entity belongs in the continuum of trust ranging from distrust to undistrust to untrust to trust using his fuzzy-logic-based trust inference rule.

Experience is used as a metric to measure trust. Griffiths [2006] also introduces a metric to measure experience based on whether the entity's expectation is met or not, which determines positive or negative experience. Each entity i can compute its experience in trust dimension d as

$$Experience_\alpha^d = \frac{I_i^{d+} - I_i^{d-}}{I_i^{d+} + I_i^{d-}}. \tag{11}$$

I_i^{d+} and I_i^{d-} refer to the number of interactions in which entity i's expectations were met and not met, respectively. This metric may reflect the expertise of an entity. For example, this formula can explain the level of expertise in d trust dimension an entity i has, such as whether or not entity i is an expert in wine. When we want to assess trust toward another entity, we may replace d with another entity j. Along with the level of confidence estimated, Griffiths [2006] uses the degree of positive or negative experience to infer trust of an entity in his fuzzy-logic-based trust inference rule.

Frequency is introduced to explain validity [Daly and Haahr 2009] and estimated as

$$Frequency(i, j) = \frac{f(i)}{F(i) - f(j)}. \tag{12}$$

This metric is computed based on the frequency a node[1] in i has encountered node j. $f(i)$ indicates the number of encounters between node i and node j, and $F(i)$ is the total number of encounters node i has observed. Daly and Haahr [2009] use frequency, closeness, intimacy, and similarity to evaluate social tie strength. Similarly, Trifunovic et al. [2010] use familiarity to represent trust based on the number of contacts with a target entity over the total number of contacts with all entities in the system. They called the familiarity an implicit social trust. Zhang et al. [2006] examine the key aspects affecting familiarity using prior experience about a similar object, repeated exposure, a level of processing (i.e., deep processing increases familiarity more than shallow processing), and forgetting rate (i.e., both immediate- and long-term delays decrease familiarity).

[1]In this work, we use the term "node" interchangeably with the term "entity" as a node is a common term to indicate an individual entity, either a human or a machine, in communication, information, and social networks.

Certainty is a determinant to discern whether trust is needed in a given context [Jøsang 2001; Wang and Singh 2010; Sun et al. 2006]. Blasch [1999] derives *confidence* for a target based on certainty, which can be defined against *uncertainty*. He defines *confidence* (C) as

$$C = 1 - U = 1 + B - PL, \quad \text{where } U = PL - B. \tag{13}$$

Here, U is *uncertainty*, PL is *plausibility*, and B is *belief*.

Leveraging DST theory [Shafer 1976], Jøsang [2001] derives trust in an opinion toward proposition x in three-tuple: belief (b_x), disbelief (d_x), and uncertainty (u_x). He defines uncertainty (u_x) as

$$u_x = 1 - b_x - d_x. \tag{14}$$

Although certainty as $1 - u_x$ does not mean trust, Jøsang et al. [2006] see trust as an *expectation* where uncertainty can be converted to trust to some extent based on prior trust toward proposition x. When an opinion w_x is denoted as $w_x = (b_x, d_x, u_x, a_x)$, where a_x is the base rate representing prior trust about proposition x, Jøsang et al. [2006] calculate the expected probability of the opinion as

$$E(w_x) = b_x + a_x u_x. \tag{15}$$

Unlike Jøsang [2001], Wang and Singh [2010] define an agent's trust based on "how strongly the agent believes that this probability is a specific value" regardless of the largeness of the value. They formulate the strength of a belief with "a probability density function of the probability of a positive experience." This is termed a Probability-Certainty Density Function (PCDF). Let $p \in [0, 1]$ be the probability that a positive result comes out. p is distributed as a function of $f : [0, 1] \to [0, \infty)$ such that $\int_0^1 f(p)dp = 1$. The probability of a positive outcome lying in $[p_1, p_2]$ can be obtained by $\int_{p_1}^{p_2} f(p)dp$, where f is the uniform distribution over probabilities p. The uniform distribution has a certainty of 0, meaning complete uncertainty. Assuming that trust of an agent is correlated with the degree it deviates from uniform distribution (i.e., additional knowledge is acquired), the mean absolute deviation (MAD) is computed to derive the certainty obtained in the interval [0, 1] by [Wang and Singh 2010]

$$c_f = \frac{\int_0^1 |f(p) - 1|dp}{2}. \tag{16}$$

Since the mean value of a PCDF is 1, as more knowledge is learned, the probability mass changes such that if $f(p)$ increases above 1 for some values of p, this will show below 1 for other values of p. Both an increase and a reduction from 1 are obtained by $|f(p) - 1|$, and $\frac{1}{2}$ is used to remove the double counting. More details are provided given positive and negative evidence in Wang and Singh [2010].

Treating trust as the opposite of uncertainty, Sun et al. [2006] estimate trust based on Shannon's entropy [1948]. Where A is a subject, i is an agent, and φ is an action, $T(A : i, \varphi)$ is the trust A has on i who will perform action φ. $P(A : i, \varphi)$ is the probability that agent i will perform φ based on subject A's perspective. $H(p)$ indicates the uncertainty based on the entropy, and the uncertainty-based trust is given by

$$T(A : i, \varphi) = \begin{cases} 1 - H(p) \text{ if } 0.5 < p \leq 1 \\ H(p) - 1 \text{ if } 0 \leq p \leq 0.5 \end{cases}$$

$$H(p) = -p \log_2(p) - (1 - p) \log_2(1 - p) \text{ where } p = P(A : i, \varphi). \tag{17}$$

When $p = 1/2$, uncertainty is the maximum with $T = 0$.

Blasch et al. [2013, 2014] propose the *Uncertainty Representation and Reasoning Evaluation Framework* (URREF) by defining information trust based on reliability and credibility in order to represent measures of uncertainty. This framework is a comprehensive ontology, aligned with standards such as the NATO Standardization Agreement (STANAG) 2511. We discuss *reliability* and *credibility* in detail next.

Reliability indicates trust in a source of information in that the source exhibits consistent behavior [Blasch et al. 2013]. In measuring reliability of a machine, based on the assumption that a failure rate arrives based on exponential distribution, reliability of a system has been commonly measured as [Blasch et al. 2013]

$$R(t) = \int_t^{\infty} \lambda e^{-\lambda x} dx = e^{-\lambda t}, \tag{18}$$

where λ is a failure rate with the exponential interarrival time and t is time. Thus, reliability decreases over time and in proportion to increase of the failure rate. The concept of reliability has been extensively used in measuring the reliability of a serial system based on the product of each component as [Mahoney et al. 2005]

$$R_{series}(t) = \prod_i^n R_i(t) = e^{-\lambda t} \text{ where } \lambda_{series} = \sum_i^n \lambda_i. \tag{19}$$

Although the reliability metric can be defined in software or hardware, reliability refers to competence of an entity in other network domains such as reliability in a human entity.

Availability indicates the system uptime. This is different from system reliability, although these two metrics are used as the same with no repair (recovery) mechanism [Heddaya and Helal 1996]. Availability of a system at time t with the repair mechanism is measured by

$$A(t) = R(t) + (1 - R(t))(1 - R(t - T_r)). \tag{20}$$

T_r is the mean time to system repair (MTTR) representing the time taken to repair the system so the system can be up again. $R(t)$ is reliability that captures the mean time to failure (MTTF) over the system time (i.e., uptime plus downtime).

Dependability has been used to indicate either reliability or availability in system performance analysis. However, there exist the cases where the two metrics do not overlap. For example, the system is up but cannot provide services properly because it is not ready for service provision. This means that the system is available but not reliable. On the other hand, the system provides reliable service during a certain period of time but is frequently interrupted by downtime. This is the case where the system is reliable but not available. In analogy with a human entity in social networks, if a person is reliable but not available or vice versa, the person cannot be used to perform a task. Heddaya and Helal [1996] combine these two metrics to devise a dependability metric as

$$D(t) = R(t)A(t). \tag{21}$$

The dependability metric measures that the system meets both conditions of the two metrics.

Competence is one of the key factors in the concept of trust. Marsh [1994] shows three states of knowledge about the competence of a trustee: (1) when the trustee is not known in any situations, (2) when the trustee is known in other situations but not this situation, and (3) when the trustee is known and trusted.

The first state represents when no information exists about the trustee. In this case, the only perceived measure to use is the disposition of a trustor and importance of the

situation. When a task to be performed is highly important, the trustor is more likely to expect higher trust in the trustee, or vice versa. The *perceived* competence of trustee j that trustor i has can be formalized by

$$Perceived\_Competence(i, j) = T(i, j)M(i, \alpha), \tag{22}$$

where i is the basic trust of trustor i in any trustees and $M(i, \alpha)$ is the importance of situation α to trustor i.

The second state explains when trustor i does not know how the trustee j performs in a certain situation but knows about trustee j in other past situations. Thus, trustor i cannot use his or her past experience with trustee j in other situations. The competence that trustor i perceives in trustee j in situation α can be estimated by

$$Perceived\_Competence(i, j, \alpha) = \frac{1}{|B|} \sum_{\beta \in B, \alpha \notin B} Experienced\_Competence(i, j, \beta)^{t'} \widehat{T(i, j)}. \tag{23}$$

Here, B refers to the set of situations βs except situation α. $Experienced\_Competence(i, j, \beta)^{t'}$ is the competence that trustor i has experienced with trustee j in other β situations in the past (time $t' < t$, where t is a current time). $\widehat{T(i, j)}$ is the general trust of trustor i in trust j.

The third state explains when trustee j is known and trusted since trustor i has interacted with trustee j in identical or similar situations α. The competence that trustor i perceives in trustee j in all situations αs can be given by

$$Perceived\_Competence(i, j, \alpha) = \frac{1}{|A|} \sum_{\alpha \in A} Experienced\_Competence(i, j, \alpha)^{t'}. \tag{24}$$

A is the set of all similar or identical situations αs.

Honesty (or integrity) is measured as one of the trust dimensions and used as the criterion to provide an incentive when nodes behave in the system, complying with the system protocol [Minhas et al. 2010]. Chen et al. [2010] use honesty as a component of overall trust indicating the maliciousness (e.g., packet dropping or lying) of an entity. Similarly with the computation of "experience" earlier, honesty is computed based on the frequency of correct operations, such as the number of packet forwarding or reporting truthful information over the total number of events that occurred related to the honesty factor [Chen et al. 2010].

Recency is used to estimate the freshness of trust relationships. Daly and Haahr [2009] use the recency metric that refers to the time duration between when node i met node j and node i has been in the network, denoted as $rec(j)$, over the total duration node i has been in the network, denoted as $L(i)$. This implies how long node i has not seen node j after it met node j last time. The recency is computed by Daly and Haahr [2009] as

$$Recency(i, j) = \frac{rec(j)}{L(i) - rec(j)}. \tag{25}$$

Keung and Griffiths [2008] compute recency as trust decays over a fewer number of recent interactions between two entities. Similarly, Huynh et al. [2006] estimate a recency function to rate trust evidence as

$$Recency(t_k, t) = \mathrm{e}^{-\frac{t - t_k}{\lambda}}. \tag{26}$$

t is the current time and t_k is the time when evidence k is recorded. The parameter λ is to rate recency to scale time values. Wen et al. [2010] also introduce a longevity factor to weigh past information and current information.

Stability has been used to represent one aspect of trust systems. Kittur et al. [2008] examine the stability of *Wikipedia* to evaluate its trustworthiness in terms of how much an article has been changed since the last viewing. Zhang et al. [2006] use the stability metric to measure trust of the system based on the trustworthiness rankings of sellers. Adomavicius and Zhang [2010] use the stability metric to measure the performance of recommendation systems based on the difference between performance predictions. Peng et al. [2008] consider stability based on the changes made between two time points by

$$Stability_i(t_{k-1}, t) = \lambda NCR_i(t_{k-1}, t) + (1 - \lambda)P_i(t_{k-1}, t). \tag{27}$$

$NCR_i(t_{k-1}, t)$ is the neighbor change ratio and $P_i(t_{k-1}, t)$ is the self-status (e.g., residual power) change ratio occurring during $t - t_{k=1}$. λ is a parameter to weigh the neighboring status, while $(1 - \lambda)$ is a parameter to weigh the self-status.

Credibility is believability in information content including veracity, objectivity, observational sensitivity, and self-confidence [Blasch et al. 2013]. Credibility in information is measured based on the level of uncertainty, which is observed with conflicting, incomplete, and/or lacking evidence. Various belief models [Shafer 1976; Dezert and Smarandache 2004; Zadeh 1983; Jøsang 2001] have been used to estimate certainty in information. In addition, social media data (e.g., Twitter, Facebook) have been popularly used to study information credibility based on other statistical methods such as maximum likelihood and feature-based methods [Castillo et al. 2011; Sikdar et al. 2014].

Completeness means whether the provided information is sufficient to provide answer(s) for the question of interest [Blasch et al. 2013]. Dutta-Bergman [2004] examines the effect of information completeness as one of the key factors that affect information credibility in medical advice websites. Ballou and Pazer [2003] study the tradeoff between data completeness and data consistency, where data completeness is defined as the "presence of all defined content at both data element and data set levels." They measure the overall completeness of data (CP) as

$$CP = \sum_{i=1}^{N} w_i cp_i, \tag{28}$$

where there exists N categories to meet data completeness and w_i is a weight to consider cp_i.

Relevance of information is used to assess trust based on four components: recency, amount of interactions, confidence of a trustor in a source of information (recommendation), and influence of a recommendation [Keung and Griffiths 2008]. It is measured by

$$Relevance^m_{k,j} = f\left(Rec^m_k, I^m_{k,j}, C^m_{k,j}, IF^m_{k,j}\right). \tag{29}$$

Rec^m_k is the recency of the recommendation by entity k on task m, $I^m_{k,j}$ indicates the amount of interactions between entities k and j on task m, $C^m_{k,j}$ is the degree of confidence that entity k has in entity j on task m, and $IF^m_{k,j}$ is the relative degree of influence of the recommendation provided by entity k about entity j on task m.

Velloso et al. [2010] use maturity to assess qualifications of recommenders for trust evaluation. They pick relevant neighboring nodes to collect recommendations based on how long a neighboring node has relationships with a target node to assess its trustworthiness. Lana and Westphall [2008] also compute maturity to assess trustworthiness of an entity in grid computing based on history of resource utilization, seniority (grid membership time), frequency of resource usage, user evaluation by the administrator, and the initial trust level a user has in the grid.

Cooperation is discussed as a threshold to determine whether an entity is cooperative or not. Marsh and Briggs [2009] define the cooperation threshold as

$$Th^{cooperation}(i, j, \alpha) = \frac{Risk(i, j, \alpha)}{Competence(i, j, \alpha) + \widehat{T(i, j)}} \times M(i, \alpha). \quad (30)$$

$Competence(i, j, \alpha)$ refers to the cooperation threshold that i has toward j in situation α. This threshold is proportionally affected by the risk entity i perceives as well as adversely affected by the competence entity i perceives toward entity j when trusting j in situation α. Further, the previous high trust between i and j, $\widehat{T(i, j)}$, may relax this threshold, while the importance of situation α to i will raise the threshold to determine cooperation with j. This formula is backed up by recent existing work that uses the concept of "social selfishness" in routing by nodes in sensor or mobile ad hoc networks [Li et al. 2010; Trifunovic et al. 2010]. That is, a node may forward a packet received from another node that has had past interaction with itself, called *social tie* [Li et al. 2010] or *friendship* [Trifunovic et al. 2010].

The cooperative behaviors can be derived differently depending on which network layer is considered. For example, in communication networks, packet dropping or forwarding behavior is used to estimate cooperative behavior of a node. In information networks, whether sharing information or not would reflect an aspect of cooperative behaviors. In social networks, prompt and/or frequent email replies can be regarded as cooperative behavior. Further, a cognitive entity with unique cognitive characteristics will be affected by its own disposition or propensity (e.g., tolerance or acceptance level) to determine its cooperative behavior. This factor may be considered in estimating $\widehat{T(i, j)}$ as earlier.

Rationality is extensively studied in the area of game-theoretic approaches and multiagent systems (MASs) where an agent is viewed as a self-interested entity to maximize its own interest (or utility). Doyle [1997] defines "rational decision making" as "choosing among alternatives in a way that properly accords with the preferences and beliefs of an individual decision maker or those of a group making a joint decision."

Market-based or game-theoretic approaches have been applied in trust systems or trust management schemes to enforce an agent to exhibit rational behavior by utilizing reward or penalty [Chin 2009; Lin and Huai 2009; Liang and Shi 2010; Wu et al. 2010]. Based on rational trust, the trustor can derive its decision (D) that maximizes its utility $U(a)$, where a is a chosen alternative, computed by

$$D = \max[U(a_1), \ldots, U(a_i) \ldots U(a_j)]. \quad (31)$$

Even if decision makers intend to make rational decisions, they often fail due to their inherent cognitive limitations and/or time constraints [Jones 1999]. This is called "bounded rationality" wherein in market-based systems it is mostly assumed that only local information is considered for decision making [Huang and Nicol 2009].

4.1.2. Emotional Trust.

Expectation is defined as epistemic representations about the future, which is more than just prediction [Castelfranchi and Falcone 2010]. Expectation is a preprocess to formulate prediction. Given that entity i has belief at time t_1, $B_i^{t_1}$, entity i has an expectation p at time t_1 that it will be true at time t_2 with the goal, $G_i^{[t_1,t_3]}$, to predict whether or not p is true for $[t_1, t_3]$, where $t_1 < t_2 < t_3$:

$$Expectation_i^p = B_i^{t_1}(p^{t_2}, True) \ \wedge \ G_i^{[t_1,t_3]}(p^{t_2}, True/False). \quad (32)$$

Beliefs have strength in terms of a degree of subjective certainty. Goals have a level of subjective importance for the agent. In sociocognitive models of trust, anxiety tends

to be greater when the goal has high importance under high uncertainty. On the other hand, when the goal is not very critical under high certainty, anxiety is low [Castelfranchi and Falcone 2010]. Expectations can be expressed as positive or negative indicating the so-called hope or fear in our daily lives, to be discussed next.

Hope is a feeling that expresses a positive expectation when the chance is rather low or uncertain with the goal that expectation p happens [Castelfranchi and Falcone 2010]. The hope of entity i can be expressed by

$$Hope_i^p = B_i^{t_1}(p^{t_2}, True)^{low} \quad \wedge \quad G_i^{[t_1,t_3]}(p^{t_2}, True)^{high}. \tag{33}$$

Fear is a feeling to expect a negative outcome under an uncertain situation where an important goal should be achieved and is formatted as [Castelfranchi and Falcone 2010]

$$Fear_i^p = B_i^{t_1}(p^{t_2}, True) \quad \wedge \quad G_i^{[t_1,t_3]}(p^{t_2}, False). \tag{34}$$

When expectation p turns out to be wrong, we call the expectation "invalidated." The invalidated expectation can be formalized as

$$Invalid\_Expectation_i^p = B_i^{t_1}(p^{t_2}, True) \quad \wedge \quad B_i^{t_3}(p^{t_2}, False), \tag{35}$$

where $t_1 < t_2 < t_3$.

Frustration occurs when an expectation is invalidated [Castelfranchi and Falcone 2010] and is formulated by

$$Frustration_i^p = G_i^{[t_1,t_3]}(p^{t_2}, True/False) \quad \wedge \quad B_i^{t_3}(p^{t_2}, False), \tag{36}$$

where $t_1 < t_2 < t_3$. Frustration is a feeling that occurs when a positive expectation turns out to be wrong.

Disappointment expresses frustration when a positive expectation, hope, is invalidated [Castelfranchi and Falcone 2010] and can be expressed as

$$Disappointment_i^p = G_i^{[t_1,t_2]}(p^{t_2}, True) \wedge B_i^{t_1}(p^{t_2}, True) \wedge B_i^{t_2}(p^{t_2}, False), \tag{37}$$

where $t_1 < t_2$. When a negative expectation turns out to be wrong, we call it relief.

Relief happens when the prediction was wrong but the goal is achieved with surprise [Castelfranchi and Falcone 2010]. Where $t_1 < t_2$, the relief can be formulated by

$$Relief_i^p = G_i^{[t_1,t_2]}(p^{t_2}, False) \wedge B_i^{t_2}(p^{t_2}, True) \wedge B_i^{t_2}(p^{t_2}, False). \tag{38}$$

Disposition is discussed to explain trusting behavior in terms of three states [Marsh 1994]: optimistic, pessimistic, and realistic. An agent estimates trust differently depending on its disposition. In distributed artificial intelligence (DAI), Marsh [1994] describes the spectrum of realism where pessimists are less likely to be forgiving or trusting in others while optimists are more likely to be forgiving or trusting in others. Here is the formula explaining "the trust of i (trustor) in j (trustee) in the situation α" that considers the disposition of an agent:

$$T(i, j, \alpha) = T(i, j)\, U(i, j, \alpha)\, M(i, \alpha), \tag{39}$$

where $T(i, j)$ estimates how much i can trust j based on the disposition of i. $U(i, j, \alpha)$ is the utility that i gains by trusting j at situation α, and $M(i, \alpha)$ estimates the importance of situation α to i. $T(i, j)$ can be different depending on the disposition of the trustor i. Trust can be differently assessed on three types of dispositions, realism, optimism, and pessimism, as

$$\widehat{T^{realism}(i, j)} = \frac{1}{|A|} \sum_{\alpha \in A} T(i, j, \alpha) \tag{40}$$

$$\widehat{T^{optimism}}(i, j) = \max_{\alpha \in A} T(i, j, \alpha) \tag{41}$$

$$\widehat{T^{pessimism}}(i, j) = \min_{\alpha \in A} T(i, j, \alpha). \tag{42}$$

$\widehat{T^{realism}}(i, j)$ explains the trust realist i can compute, where A indicates a set of situations such as all situations, situations in which agent i is involved with agent j, and/or similar situations agent i experienced (e.g., met an agent similar to agent j). $\widehat{T^{optimism}}(i, j)$ and $\widehat{T^{pessimism}}(i, j)$ show the trust computation where agent i is an optimist or pessimist. Since a different trust will be required in a different situation, there are variants to compute the trust of agent i in agent j in different situations based on its disposition or propensity [Marsh 1994].

Marsh [1994] points out the memory span in which an agent can maintain an amount of information on past experience. Willingness to trust is related to the attitude to take risks. In the commercial vehicle industry, Kalnbach and Lantz [1997] study how optimistic attitudes and willingness to trust can affect performance of workers in task performance.

Regret is regarded as a critical factor in trust. Luhmann [1979] says that "trust is only required if a bad outcome would make you regret your decision." We often regret something that happened or something we have done in the past. Regret can be used to reduce a similar negative experience from happening again [Marsh and Briggs 2009]. In modeling regret, Marsh and Briggs [2009] concern three questions to answer: "what was lost (κ), what is meant (λ), and how it feels (μ)." Trustor i's decision to trust trustee j puts i to regret when i is betrayed by j. The Marsh and Briggs [2009] regret function is formulated as

$$Regret(i, j, \alpha) = U(i, j, \alpha) - U(i, j, \bar{\alpha})) \bullet f(\kappa, \lambda, \mu), \tag{43}$$

where $\bullet$ denotes some operation (e.g., multiplication), i is an entity, and α is a particular situation. $U(i, j, \alpha)$ is the gain from the original estimation (i.e., could have been gained) of what is expected to happen and $U(i, j, \bar{\alpha})$ is the actual gain from what really happened. $f(\kappa, \lambda, \mu)$ is a personal meaningfulness function that considers the three factors mentioned previously. This function can be further refined depending on three scenarios: "I regret that you did that," "you regret that you did that," and "I regret that I did not do that." $f(\kappa, \lambda, \mu)$ can particularly consider the importance of trust relationship between two entities, the degree of perceived risk of the trust relationship, the degree of being deprived from what happened, and miscalculation of the importance of the trust relationship in a particular situation [Marsh and Briggs 2009].

4.2. Relational Trust Attributes

Sociologists have perceived trust as an attribute of collective units, not limited to only an attribute of an individual entity [Luhmann 1979; Barber 1983; Lewis and Weigert 1985]. In computing research areas, trust has been recognized to indicate the quality of relationships among entities in social networks or reputation systems [Zieglera and Golbeck2007]. Characteristics defining relationships between entities such as individuals, organizations, and/or groups have been considered to define so-called social trust. In this section, we discuss factors by which an entity is affected by trust relationships or decision making such as similarity, centrality (betweenness), and importance.

Similarity of users in online applications is popularly computed using the Pearson correlation coefficient [Breese et al. 1998]. The similarity of two users is obtained by

comparing the ratings provided by the two users as

$$Similarity_{rating}(\alpha, \beta) = \frac{\sum_{i \in G}(r_{\alpha,i} - \hat{r_\alpha})(r_{\beta,i} - \hat{r_\beta})}{\sqrt{\sum_{i \in G}(r_{\alpha,i} - \hat{r_\alpha})^2 \sum_{i \in G}(r_{\beta,i} - \hat{r_\beta}))^2}}. \quad (44)$$

Here, α and β are two different users and i is any user that belongs to a set G including all users in the system except users α and β. $r(\alpha, i)$ refers to the rating evaluated by α about user i.

In social networks, similarity is often measured based on the neighbors both nodes know. Liben-Nowell and Kleinberg [2003] define similarity using the intersection of the two neighborhood nodes, i and j, known as

$$Similarity_{neighborhood}(i, j) = |N(i) \cap N(j)|. \quad (45)$$

Daly and Haahr [2009] use the same formula to calculate similarity between two nodes, but the neighborhood is defined as a set of contacts held by each node. Bank and Cole [2008] measure similarity based on the common number of neighbors over the union of neighbors known by two parties. Adamic and Adar [2003] measure similarity of two pages, incoming and outgoing, depending on whether or not it has frequent features. Liben-Nowell and Kleinberg [2003] adopt Adamic and Adar's way to compute similarity based on common neighbors or rare neighbors. Newman [2001] predicts the probability of future collaborators in scientific communities. Liben-Nowell and Kleinberg [2003] propose their similarity metric to predict the future collaboration between two individuals.

There are abundant metrics in the literature to model centrality or influence in networks [Everett and Borgatti 2005; Bonacich 1987; Brandes 2001; Freeman 1979; Freeman et al. 1991; Goh et al. 2003; Sabidussi 1966; Hage and Harary 1995; Shimbel 1953].

Centrality or betweenness centrality has been used to represent the degree of importance or influence of an entity since the 1950s. Freeman [1977, 1979] estimates *degree centrality* based on the number of direct ties associated with a given node. Degree centrality of a given node p_i, where $a(p_i, p_k) = 1$ if p_i and p_k can communicate via direct link, is computed by

$$Centrality_{degree}^{Freeman}(p_i) = \sum_{k \in K} a(p_i, p_k). \quad (46)$$

Here, k is an element of K, a set of all nodes in the system. Freeman [1977] describes *closeness (proximity) centrality* based on the reciprocal of the "mean geodesic distance."

Closeness centrality is defined by "a measure of how long it will take information to flow from a given node to other nodes in the network" [Newman 2005] and can be computed by

$$Centrality_{closeness}^{Newman}(p_i) = \frac{|N| - 1}{\sum_{n \in N} d(p_i, p_n)}. \quad (47)$$

Here, for a given node p_i, N refers to a set of nodes who can be reached in the network by p_i.

Newman [2005] computes *betweenness centrality* based on how much a node has control in exchanging information with others. That is, if a node is more capable of facilitating interactions (or communication) among nodes it is connected with, it indicates high betweenness centrality [Newman 2005]. Where $g_{i,k}$ is the number of all geodesic paths connecting p_i and p_k and $g_{i,k}(p_i)$ is the number of the geodesic paths

including p_i [Newman 2005], betweenness centrality is computed by

$$Centrality_{betwenness}^{Newman}(p_i) = \sum_{j \in J} \sum_{k \in K} \frac{g_{j,k}(p_i)}{g_{j,k}}. \quad (48)$$

Freeman's closeness centrality metric and Newman's centrality metrics (closeness and betweenness) require a node to be aware of an entire network, requiring a certain level of global review, for example, all possible paths from node i to node j to compute the number of the shortest paths between them [Daly and Haahr 2009]. This drawback introduces an "ego network," which refers to a network with a single actor (ego) that is connected with multiple actors (alters) that have links among them [Marsden 2002]. Marsden [2002] introduces centrality measures in ego networks compared to Freeman's centrality metrics. Daly and Haahr [2009] use an intimacy or closeness centrality as a component of the tie strength metric.

Importance of an entity is also examined to measure trust of the entity in a network. Shapley [1953] proposes a value to express the importance of each player in a coalition game. In this game, players cooperate and obtain a certain gain (i.e., payoff) if the coalition wins. Some players may contribute more than others. In that case, there should be a different distribution of the gains among players. The Shapley value gives how important each player's contribution is to the overall cooperation and is computed as

$$\varphi_i(v) = \sum_{S \in N, i \notin N} \frac{|S|!(n - |S| - 1)}{n!}(v(S \cup i) - v(S)). \quad (49)$$

This Shapley value indicates the amount of profits player i obtains in a given coalition game. S is a coalition of players agreeing to cooperation. n is the total number of players. N is a set of players that does not include player i. S is a subset of N and v is a function of value of a coalition.

$v(S)$ indicates the value of coalition S, which means the overall gain expected from coalition S. $v(S \cup i) - v(S)$ gives the fair amount of player i's contribution to the coalition game. The fraction with permutations averages over the possible different permutations where the coalition can be formed.

Based on the constructs of trust discussed in Sections 4.1 and 4.2, we also look into how the various constructs of trust can fit for each layer of a complex, composite network embracing communication, information, and social/cognitive domains.

4.3. Composite Trust

This work proposes the concept of composite trust characterized by communication trust, information trust, social trust, and cognitive trust that can be derived from a complex, composite network.

Communication Trust refers to trust deriving from the characteristics of communication networks in which the network consists of a number of nodes and links to connect them via cable or wireless media. Dimensions of trust in communication networks can be measured objectively and are closely related to the aspects of quality of service (QoS) such as network connectivity (e.g., k-connectedness, average shortest path, node density, reachability), fault tolerance (e.g., system lifetime), cooperative or selfish behaviors (e.g., forwarding or dropping packets), and network capacity (e.g., traffic or congestion) [Daly and Haahr 2009; Desmedt et al. 2007; Jøsang 1999; Lana and Westphall 2008; Cho et al. 2011].

Information Trust indicates trust in information networks that provide information services based on information sharing. Information trust includes multiple aspects related to quality of information (QoI) and credibility [Blasch et al. 2010]. Rieh and

Danielson [2007] point out the difference between trust and credibility. Trust is "a positive belief about the perceived reliability, dependability, and confidence on a person, object, or process based on the willingness to accept risk and vulnerability" [Rieh and Danielson 2007]. Credibility indicates "a perceived quality of a source, which may or may not result in associated trusting behaviors" [Rieh and Danielson 2007]. The dimensions of credibility or QoI include "quality, authority, reliability, validity, trustworthiness, and expertise of a source, in addition to relevance, consistency, recency, and correctness" [Rieh and Danielson 2007]. Hilligoss and Rieh [2008] define the constructs of credibility as "trustfulness, believability, trustworthiness, objectivity, reliability, trust, accuracy, and fairness." Most researchers agree on the salient features of credibility as trustworthiness and expertise to ensure honesty and reliability in both source and information.

Social Trust indicates trust between humans in social networks. A social network is a network structure consisting of individuals or organizations formed based on ties between them. According to Golbeck [2009], social trust is a fuzzy concept observed in social trust relationships between people. Social trust between two individuals is studied by examining interaction history; similarity in preferences, background, and demographics; reputation or recommendations obtained from third parties; different life experiences of individuals; and so forth. Recently many social trust researchers have used data from social networking applications to investigate the trust relationships between people and to examine critical factors that affect relationships. However, online relationships are usually different from those in real life in that people may be generous in maintaining relationships in online social networks (e.g., Facebook, Twitter, LinkIn, etc.), while those relationships may not exist offline [Golbeck 2009].

Cognitive Trust refers to trust derived through cognitive reasoning, where cognition is the process of thoughts, mental functions, or mental processes as the state of intelligent entities [Wikipedia 2015]. Johnson and Grayson [2005] discuss cognitive trust in relationships between a service provider and a customer. The author describes that cognitive trust refers to "confidence or willingness of customers to rely on a service provider's competence and reliability" [Johnson and Grayson 2005]. Usually the cognitive trust comes from accumulated knowledge to make predictions but with uncertainty for possible risk. In a complex network that has human entities involved, the entity's cognitive motivations and/or competence affects their way of information processing and accordingly affects trust assessment toward interacting parties.

In the area of artificial intelligence and human–machine interaction, the concept of cognitive trust follows as the reasoning process in mental functions. Accordingly, cognitive trust can be measured by assessing emotional and reasoning aspects of human thoughts such as expectation, hope, belief, frustration, disappointment, disposition, maturity, willingness, rationality, and regret.

As an example of composite trust, in the human–machine research area, there have been efforts to define trust in automation in terms of composite characteristics of an entity. Muir [1994] elaborates the concept of trust based on expectation [Barber 1983] and experience [Rempel et al. 1985]. Muir [1994] categorizes *expectation* in terms of persistence, technical competence, and fiduciary responsibility using the dimensions of trust proposed by Barber [1983]. Muir [1994] defines trust of a supervisor toward a human or machine by combining the previous three components as

$$T_i = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_1 X_2 + \beta_5 X_1 X_3 + \beta_6 X_2 X_3 + \beta_7 X_1 X_2 X_3. \quad (50)$$

β_{0-7} are parameters, X_l is "persistence," X_2 is "technical competence," and X_3 "fiduciary responsibility." This formula shows that there exist dimensions of interdependency between the three components.

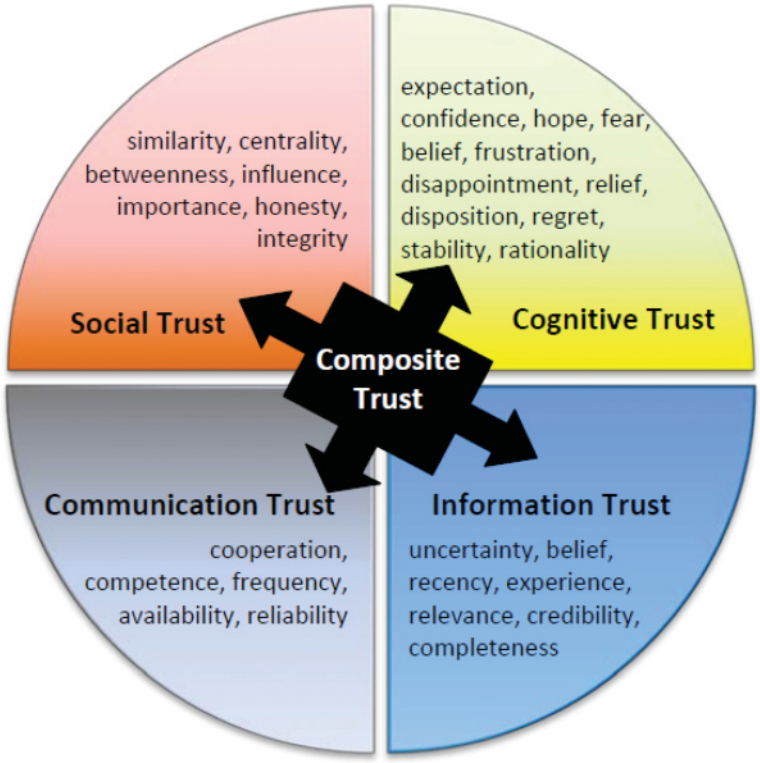


Fig. 5. Dimensions of trust in a composite network.

Muir [1994] further analyzes *expectation* according to the different levels of *experience* in terms of predictability of an act, dependability of dispositions, and faith in motives proposed by Rempel et al. [1985]. Muir [1994] proposes that the three different levels of experience can be the basis of estimating expectation as the core concept of trust. Considering the six components, they define trust as

$$\begin{aligned} Trust \;=\; & Predictability + Dependability + Faith \\ & + Competence + Responsibility + Reliability. \end{aligned} \tag{51}$$

Reliability refers to the fiduciary responsibility based on the model by Barber [1983].

Figure 5 shows how the various constructs of trust discussed in this section are related to the different dimensions of composite trust. The concept of a composite network implies that an entity belongs to different types of networks, which may include communication, information, and social network, where the entity has the cognitive ability to make intelligent decisions. For example, we humans communicate to each other through various mediums of communication networks (e.g., phones, emails, social media) and make and maintain social relationships with other people. The relationship can be maintained or broken based on the perceived trust toward each other, which is related to the concept of cognitive trust. To ensure trust toward another entity, we use information that may not always be perfect or certain and so we need to derive credible, relevant, fresh information with uncertain, incomplete, and conflicting evidence. In this example, we recognize how an entity's trust toward another entity can be interwoven based on the interplay of the characteristics of different layers of the complex, composite network.

5. PROPERTIES OF TRUST

In this section, we discuss the following key trust properties and how they are applied in the literature: subjectivity, dynamicity, asymmetry, transitivity, and context dependency.

5.1. Subjectivity

Subjectivity is the inherent nature of trust in which objective trust assessment may not be possible where evidence may be uncertain, incomplete, and conflicting in reality. Note that subjective trust implies estimated trust based on local, uncertain, and/or incomplete evidence, while objective trust refers to a ground-truth trust that uses an *oracle* with global information. Of course, estimating objective trust is not possible in reality. In particular, subjective trust is inferred through the cognitive reasoning process affected by the entity's disposition [Hasan et al. 2009] and/or personal preference [Yan et al. 2003].

In the philosophical sense [Porter 1995], the objectivity of science generally means the ability to know things as they really are. However, in a regime of trust, subjective discretionary decisions can bring far more useful results than objective indiscriminate decisions with uncertain, incomplete evidence [Porter 1995].

Porter's view on the superior aspect of decisions by subjective discretion can be supported by Jøsang's two types of trust [2005]: (1) *reliability trust* is a context-independent trust based on reliability perceived by an observer, which is orthogonal to given situations and recognizes possible risk, representing objective trust; and (2) *decision trust* is a context-dependent trust that gives relative reliance in given situations despite that negative results may be generated. However, in some contexts, the context-dependent situational trust may be needed to achieve a given task even under high risk. That is, trust estimates based on subjective discretion can bring positive results depending on the situation. By the same token, Blaze et al. [2009] discuss that situational dynamism should be considered in trust management where even less reliable information or results can critically contribute to the success of a given task.

The subjective aspect of trust has been studied by fuzzy set theory treating subjective trust as a belief [Zadeh 1965]. Ma et al. [2010] use "fuzzy comprehensive evaluation" to estimate trust using credit and reputation. Hasan et al. [2009] propose a method to eliminate the subjectivity of trust. Marsh [1994] uses memory span to consider the disposition of agents to measure subjective trust in multiagent systems.

5.2. Dynamicity

Dynamicity of trust is intrinsic in its nature [Castelfranchi and Falcone 1998a]. Trust evolves over time based on the types of experiences or the amount of interactions. Trust is affected by the fluctuations of a trustor's or trustee's emotional or rational status. In addition, trust is affected by different social contexts. For example, trust is influenced by the existence of authority/control entities, the characteristics of given tasks, and/or the nature of contracts (e.g., rules, regulations, or laws). Although in human-to-machine trust the dynamics of trust are emphasized due to the dynamic nature of human entities, even machine-to-machine trust may not be *static* because a node's resource may decay or be compromised by an attacker over time.

Trust decays over time and is updated upon the arrival of new evidence. Jøsang et al. [2006] suggest modeling the decay of trust when entity i assesses entity j's trust at time t as

$$T(i, j, t) = \lambda^{t-t_r} T(i, j, t_r). \tag{52}$$

Note that $0 \leq \lambda \leq 1$ and t_r is the time at which the rating was collected and t is the current time. In particular, this formula can be used when no new information or only part of trust at current time t is available. Dynamicity of trust has been studied by considering trust decay over time or space [Cho et al. 2009], experiences/interactions [English et al. 2003; Marsh 1994], or decision making under different context or situations [Blaze et al. 2009].

5.3. Asymmetry

Asymmetry of trust addresses how two entities do not necessarily have equal degrees of trust toward each other. This may be affected by asymmetric characteristics of two parties to establish a trust relationship. Asymmetric characteristics may include nonsymmetrical situations between actors, power (e.g., authority), different cultures, or resources. In this context, asymmetry can be regarded as difference in knowledge, power, and culture of actors [Blomqvist and Stahle 2000]. Asymmetric trust relationships can be mitigated to some extent by the reciprocal (or reciprocation) nature of the dyadic relationship. That is, as A trusts B more over time, B becomes trusting of A more as well. This reduces the gap of asymmetry in trust between two nodes, leading to a symmetric trust relationship. This can be modeled by an undirected graph such that if A trusts B, then B trust A as well.

Cvetkovich et al. [2002] and Slovic [1993] discuss asymmetry of trust in information. They claim that trust-destroying (negative) events impact more than trust-building (positive) events in trust judgment, emphasizing the fragility of trust. Kramer [1999] examines asymmetries of trust behaviors depending on individuals' positions within a hierarchical relationship. The asymmetry characteristic of trust is applied in networking research to develop secure networking protocols [Dinda 2004; Desmedt et al. 2007].

5.4. Incomplete Transitivity

Incomplete transitivity of trust is observed in reality, although perfect trust transitivity is addressed in cryptography such as PGP (Pretty Good Privacy) using the concept of the web of trust. In the *web of trust*, if there is a trust chain from A to B and from B to C, then A also trusts C as much as B trusts C [Stallings 1995]. Luhmann [1979] insists on nontransitivity of trust in that "Trust is not transferable to other objects or to other people who trust." In particular, this case occurs when two entities have totally different knowledge bases, so they may have conflicting opinions toward a same entity or object. As a conservative perspective, most trust researchers reach a consensus in that trust is not completely transitive or transferable to another entity particularly when humans are in the loop of a system.

Jøsang [2003, 2005] discusses that under certain semantic constraints, trust can be partially transitive. He discusses referral trust and functional trust, where the former is the ability to refer to a third party, while the latter is the ability to recommend the third party based on a direct relationship. Alice can refer to Bob's recommendation about another referral person, Claire, who has direct experience with a car mechanic, David. Alice has a referral trust in Bob, Bob has a referral trust in Claire, and Claire has a functional trust in David. Trust is not completely transitive based on human perceptions and is diluted through transitivity. In this example scenario, we can say that Alice can trust David as much as Claire trusts David at most.

Marsh [1994] backs up the incomplete transitivity of trust. For rational entity x, the following may hold as

$$T(x, y) > T(x, z) \quad \wedge \quad T(x, z) > T(x, w) \Rightarrow T(x, y) > T(x, w). \tag{53}$$

Table V. Trust Properties in the Process of Trust Assessment in Figure 1

Trust Property	Phase in Trust Assessment
Subjectivity	Individual (emotional and logical) and relational trust assessment
Dynamicity	Uncertainty and ambiguity analysis due to dynamics in risk assessment
Asymmetry	Vulnerability and impact analysis in risk assessment
Incomplete Transitivity	Enhancing situation awareness by propagating proven trust evidence (i.e., feedback based on trustworthiness) through a trust chain
Context Dependency	Vulnerability, impact, and utility analysis in risk assessment

The notation $T(x, y)$ represents trust of x in y. However, trust is not transitive in any relation as

$$T(x, y) > T(y, w) \quad \not\Rightarrow \quad T(x, y) > T(x, w). \tag{54}$$

Marsh [1994] describes that "x trusts y by some amount and y trusts w by some other amount does not say about how much x trusts w." Dondio et al. [2008] propose a compatibility scheme of trust between systems with different trust schemes. They use the degree of compatibility to weigh exchanged trust judgment based on the incomplete transitivity of trust.

Although trust cannot be completely transitive, trust can be easily transferred from one context (personal friendships) to another context (business relationships) [Bradach and Eccles 1989]. The idea of trust transferability has been adopted in many business settings [Lewicki and Bunker 1995; Lin and Lu 2010].

5.5. Context Dependency

Context dependency of trust helps derive critical factors to estimate trust in a given context. For example, Bob is a good physician, but he may not be a good car mechanic [Jøsang and Pope 2005]. Investigating the given context helps derive trust to achieve the goal of trust assessment. In addition, as discussed in Section 5, given a situation, *reliability trust* is a *context-independent*, objective trust, while *decision trust* is a *context-dependent*, subjective trust [Jøsang and Pope 2005]. But oftentimes we choose a context-dependent decision trust because whether to trust or not affects the outcome of goal achievement.

The context dependency of trust has been modeled in various domains including trust and reputation systems [Malacka et al. 2010], pervasive collaborative environments [Corradi et al. 2005], and organizational management [Mayer et al. 1995].

5.6. Trust Properties in Trust Assessment

In Figure 1 of Section 2.2, we described the process of trust assessment in detail. We associate each phase of trust assessment described in Figure 1 with each property of trust discussed in this section. Key dimensions of trust in individual and relational levels are estimated subjectively. The dynamics of relationships or a system generate uncertain, incomplete, or conflicting evidence, which should be considered to estimate the level of uncertainty and ambiguity. Since two entities trust each other to different degrees, there exists potential betrayal exposing potential vulnerability, and this may result in a huge negative impact upon a trustee's betrayal. Trustworthy, proven evidence is fed back or propagated to other entities through a trust chain, leading to enhanced situation awareness by individual entities in a given system. Deciding on whether or not to trust is closely related to vulnerability, impact, and utility in a given context. Therefore, all five trust properties, at least, should be preserved in the process of trust assessment, in particular applications involving humans in the loop.

6. APPLICATIONS, CHALLENGES, AND SUGGESTIONS

6.1. Trust-Based Applications

Trust has been applied to help enhance the decision-making process in various domains. This section discusses how trust has been employed in the computing and engineering fields.

The **Artificial Intelligence (AI)** research community has been active in conducting trust research through agent modeling. Since agents are assumed to be intelligent, rational, cooperative, and independent [Marsh 1994], trust is considered as a key factor that impacts interactions between agents in distributed multiagent systems (DMASs). In DMASs, trust has been used in various applications such as service composition in web services [Hang and Singh 2010], air traffic control [Cammarata et al. 1988], open information systems [Hewitt 1991], trust/reputation systems [Huynh et al. 2006], reputation and social network analysis [Sabater and Sierra 2002], and task scheduling [Rabeloa et al. 1999].

Human–Computer Interaction (HCI) has investigated trust to create trustworthy websites or web services that can attract more users. Zheng et al. [2011] survey key factors that impact trust in human beings and computers in online contexts in terms of computer user interface (CUI), notification and visualization for trust-associated information, and trust management to maintain computer systems and communications. Trust cues are measured based on the features of interface and structure design (to improve "the look and feel" of a CUI), content design (to preserve security and privacy), and social cue design (e.g., indicators of social presence such as photographs) [Jensen et al. 2005; Wang and Emurian 2005]. Trustworthiness of information content by providing relevant and useful content to target populations is a strong trust cue [Shelat and Egger 2002]. In addition, quality of services and information provided by the computer affects users' trust and satisfaction [Lee and Chung 2009].

Data Fusion is another active research area that uses trust to enhance decision making based on various fusion techniques. Data fusion is the process that combines multiple records into a single, consistent, complete, and concise form in the presence of uncertain, incomplete, and conflicting evidence [Bleiholder and Naumann 2008]. Many works on data (or information) fusion have been proposed to deal with fusing multiple reports generated by sensors based on trust with the goal of making correct decisions [Yang et al. 2010; Nevell et al. 2010; Blasch et al. 2013]. Various theories are adopted to implement information fusion based on trust such as Kalman filtering [Matei et al. 2009], DST to minimize uncertainty in combining sensor information [Pong and Challa 2007], TBM to fuse soft information from human observers [Stampouli et al. 2010], and subjective logic to interpret and fuse information from multiple sources in different situations [Jøsang and Hankin 2012].

The **Human–Machine Fusion** research area combines HCI and Data Fusion noted earlier. Blasch and Plano [2002] propose the *Level 5 Fusion Model* considering a human's role in the fusion process in terms of monitoring and controlling. The proposed model divides sensor management into two processes, which consist of processes by both machines and humans. They show the data-feature-decision (DFD) model [Bedworth and Obrien 2000] for the machine fusion parts and the Joint Director's of Labs (JDL) model [Steinberg et al. 1999] for the human–computer interfaces.

Networking & Network Security researchers have explored the development of trust and reputation management with the goals of achieving high performance and security. The notion of trust has been used to estimate an entity's selfishness or capability for the purpose of efficient and effective resource allocation such as sensor allocation in multiagent systems [Shen et al. 2011], service composition and binding [Wang et al. 2013], and task assignment [Cho et al. 2013]. In addition, trust has been used as a soft

approach to achieve security, such as identifying malicious or selfish entities in networks. Various security applications using trust, including intrusion detection, secure routing, key management, and access control, have been studied extensively in the literature [Cho et al. 2011]. Kamvar et al. [2003] propose the EigenTrust reputation algorithm for peer-to-peer (P2P) networks to prevent fake trust value manipulation by malicious nodes. Shaikh et al. [2009] propose a trust model that assesses the trustworthiness of sensor groups in large-scale sensor networks in the presence of malicious, selfish, and faulty nodes. Baras and Jiang 2004] model a wireless network as an undirected graph based on graph theory [Diestel 2010]. Bayesian trust models are used to measure trust in pervasive computing [Quercia et al. 2006] and P2P networks [Wang and Vassileva 2003] to deal with malicious entities.

Data Mining techniques have been used for trust assessment in many applications, particularly to analyze big data such as privacy preserving based on multilevel trust [Li et al. 2012]; identifying trust, distrust, and/or privacy factors in online social networks [Fong et al. 2012; Bachi et al. 2012]; analyzing trust relationships in big data from social network applications (e.g., Facebook, Twitter) [Fong and Chen 2010; Szomszor et al. 2011]; and assessing trust based on a statistical method called logit regression to capture behavioral patterns of entities [Wang et al. 2014].

The **Automation** research community has inspired trust research in many other computing and engineering research areas since the 1990s [Lee and Moray 1992; Mayer et al. 1995]. Muir and Moray [1996] investigate the effect of operators' subjective trust and the use of the automation in a simulated supervisory process control task. Blasch and Plano [2002] also present a fusion system to support a human using the notion of trust. Moray et al. [2000] study the effect of automation reliability on an operator's subjective trust. Fan et al. [2008] conduct experiments to uncover the nature of human trust in human–agent collaboration in order to improve decisions in automation usage. The studies on humans' trust in automation have been extensively applied in modeling trust in other areas such as multiagent systems where an agent can be either a machine or a human [Castelfranchi and Falcone 1998a]. Parasuraman et al. [2008] look into how much situation awareness (SA), mental workload, and trust in automation can promote the human–system performance in complex systems.

Based on various components of trust addressed in Section 4, we suggest that various components should be primarily investigated in each domain of applications in Table VI.

6.2. Challenges and Suggestions

We have discussed a variety of applications using the concept of trust in diverse domains. Although the challenges of trust research may be unique depending on a domain, this section identifies and discusses the common design challenges and corresponding suggestions in developing trust models as follows:

—**Identification of key trust dimensions.** In any context, trust can be the basis for decision making closely related to achieving a system/application goal. Since dimensions of trust are numerous, it is not trivial to select key components of trust to maximize decision performance. Reflecting the notion of context dependency in the nature of trust, trust system designers should investigate the requirements of entities and/or information that can be directly related to achieving given goals of systems.

—**Optimal balance of multiple objectives based on situational trust.** As seen in Section 2, trust assessment is affected by many different factors particularly related to utility and risk analysis under the dynamics of a situation. Although trust can be estimated based on objective criteria, regardless of the level of objective trust, a

Table VI. Key Trust Components of Each Application Domain in a Composite Network

	Communication Trust	Information Trust	Social Trust	Cognitive Trust
Artificial Intelligence	cooperation, availability	belief, experience, uncertainty	importance, honesty	expectation, confidence, hope, fear, frustration, disappointment, relief, regret
Human–Computer Interaction	reliability, availability	belief, experience, uncertainty	importance, integrity	expectation, frustration, regret, experience, hope, fear
Data Fusion	availability	credibility, relevance, completeness, recency	source's influence and integrity	disposition (optimistic, pessimistic)
Human–Machine Fusion	competence, reliability, availability	credibility, relevance, completeness, recency	source's influence and integrity	disposition
Networking & Network Security	reliability, availability	integrity	honesty, centrality	experience (learning)
Data Mining	availability	relevance, credibility, completeness	similarity, importance	belief
Automation	reliability, availability	belief, experience	integrity, importance	expectation, confidence

binary decision should often be made to take actions under deprived conditions such as lack of resources and/or high uncertainty. That is, situational trust may be critical depending on context and balance key tradeoffs between conflicting goals in order to maximize the decision effectiveness and/or task performance.

—**Adaptability to dynamic environments in estimating trust.** The dynamics of a situation and/or network environments significantly affect trust estimation. A network may have different operational status due to mobility/failure, hostility, resource constraints, task characteristics (e.g., services, operations, interactions), and/or no trusted infrastructure. An entity should be adaptable to changing operational and/or node conditions for accurate trust estimation, which can be the basis for critical decision making.

—**Verification and validation of trust models.** Trust model verification and validation has been a grand challenge because of the inherent subjective nature of trust. Even in a social computing area, researchers insist that there is no objective social trust [Golbeck 2009]. However, in order to prove the benefit of trust models, one may want to develop a performance metric that can demonstrate the application performance optimization in proposed trust models.

—**Maximization of situation awareness to increase the accuracy of trust estimation.** Endsley [1996] defines SA as perceiving environmental factors in time and space, analyzing the meaning of the factors, and predicting their status in the near future. This implies the three levels of SA in terms of perceiving critical situational factors, interpreting them, and predicting future status for effective decision making. Since trust is often inferred based on the analysis of situational factors, trust system designers need to aim to achieve high SA, which is a critical factor in accurately estimating trust to promote effective decision making.

7. CONCLUDING REMARKS

In this work, we comprehensively surveyed multidisciplinary definitions of trust, trust-related concepts, trust representations, trust properties, and formulations of trust constructs. In addition, we discussed how to measure trust attributes from complex, composite networks consisting of communication, information, social, and cognitive domains. We addressed how trust research has been explored for various purposes in diverse research domains.

As in this modern society a network becomes more and more complex and interwoven between multiple factors, accordingly deriving trust in the network becomes highly complex. We introduced the concept of composite trust deriving from the interplay of unique characteristics of different layers of a complex network.

For proper quantification of trust in a complex, composite network, the identification of key trust dimensions in a given context or task scenario is the first step. The second step is to tackle how to formalize trust and validate trust metrics or models. Following these two steps, we can then accurately make trust assessments that can be the basis of effective decision making through maximizing situation awareness that provides accurate perception, interpretation, and prediction of critical situational factors for future decision making.

REFERENCES

S. Adalı. 2013. *Modeling Trust Context in Networks*. Springer Briefs in Computer Science.

L. A. Adamic and E. Adar. 2003. Friends and neighbors on the web. *Social Networks* 25, 3 (July 2003), 211–230.

G. Adomavicius and J. Zhang. 2010. On the stability of recommendation algorithms. In *Proceedings of the 4th ACM Conference on Recommender systems (RecSys'10)*. Barcelona, Spain, 47–54.

R. Axelrod. 1981. The evolution of cooperation. *Science* 211 (1981), 1390–1396.

G. Bachi, M. Coscia, A. Monreale, and F. Giannotti. 2012. Classifying trust/distrust relationships in online social networks. In *Proceedings of the 2012 International Conference on Social Computing/Privacy, Security, Risk and Trust (PASSAT'12)*. Amsterdam, Netherlands, 552–557.

D. P. Ballou and H. L. Pazer. 2003. Modeling completeness versus consistency tradeoffs in information decision contexts. *IEEE Transactions on Knowledge and Data Engineering* 15, 1 (Jan./Feb. 2003), 240–243.

J. Bank and B. Cole. 2008. Calculating the Jaccard similarity coefficient with map reduce for entity pairs in Wikipedia. Wikipedia Similarity Team. (Dec. 2008).

J. S. Baras and T. Jiang. 2004. Cooperative games, phase transitions on graphs and distributed trust in MANET. In *Proceedings of the 43th IEEE Conference on Decision and Control*. Atlantis, Paradise Island, Bahamas.

B. Barber. 1983. *The Logic and Limits of Trust*. Rutgers University Press, New Brunswick, NJ.

M. Bedworth and J. Obrien. 2000. The omnibus model: A new model of data fusion? *IEEE Aerospace and Electronic Systems Magazine* 15, 4 (April 2000), 30–36.

E. Blasch. 1999. *Derivation of a Belief Filter for High Range Resolution Radar Simultaneous Target Tracking and Identification*. Ph.D. Dissertation. Wright State University.

E. Blasch, A. Jøsang, J. Dezert, P. C. G. Costa, K. B. Laskey, and A.-L. Jousselme. 2014. URREF self-confidence in information fusion trust. In *Proceedings of the IEEE 17th International Conference on Information Fusion*. Salamanca, Spain, 1–8.

E. Blasch, K. B. Laskey, A.-L. Jousselme, V. Dragos, P. C. G. Cost, and J. Dezert. 2013. URREF reliability versus credibility in information fusion (STANAG 2511). In *IEEE 16th International Conference on Information Fusion*.

E. P. Blasch and S. Plano. 2002. JDL level 5 fusion model "user refinement" issues and applications in group tracking. In *Proceedings of SPIE: Signal Processing, Sensor Fusion, and Target Recognition*, Vol. 4729. 270–279.

E. P. Blasch, P. Valin, and E. Bosse. 2010. Measures of effectiveness for high-level fusion. In *Proceedings of the IEEE International Conference on Information Fusion*. Edinburgh, Scotland, 1–8.

M. Blaze, S. Kannan, I. Lee, O. Sokolsky, J. M. Smith, A. D. Keromytis, and W. Lee. 2009. Dynamic trust management. *Computers* 42, 2 (2009), 44–52.

J. Bleiholder and F. Naumann. 2008. Data fusion. *ACM Computing Surveys* 41, 1 (Dec. 2008), Article 1.

K. Blomqvist and P. Stahle. 2000. Building organizational trust. In *16th IMP International Conference*.

P. F. Bonacich. 1987. Power and centrality: A family of measures. *American Journal of Sociology* 92, 5 (March 1987), 1170–1182.

S. Boon and J. G. Holmes. 1991. The dynamics of interpersonal trust: Resolving uncertainty in the face of risk. In *Cooperation and Prosocial Behavior*, R. A. Hinde and J. Groebel (Eds.). Cambridge University Press.

P. Bourdieu. 1983. Forms of capital. In *Theory and Research for the Sociology of Education*, R. A. Hinde and J. Groebel (Eds.). Greenwood Press, New York.

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

U. Brandes. 2001. A faster algorithm for betweenness centrality. *Journal of Mathematical Sociology* 25 (2001), 163–177.

J. Breese, D. Heckerman, and C. Kadie. 1998. Empirical analysis of predictive algorithms for collaborative filtering. In *Proceedings of the 14th Conference on Uncertainty in Artificial Intelligence*. Morgan Kaufmann Publisher, Madison, WI, 43–52.

R. S. Burt. 2000. The network structure of social capital. *Research in Organizational Behavior* 22 (2000), 345–423.

S. J. Cammarata, D. J. McArthur, and R. Steeb. 1988. Strategies of cooperation in distributed problem solving. In *Distributed Artificial Intelligence*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 102–105.

C. Castelfranchi. 1995. Social commitment: From individual intentions to groups and organizations. In *Proceedings of the 1st International Conference on Multi-Agent Systems (ICMAS'95)*. AAAI-MIT Press, San Francisco, California, USA, 41–49.

C. Castelfranchi. 2009. A non-reductionist approach to trust. In *Computing with Social Trust*, J. Golbeck (Ed.). Springer, London Limited, Human-Computer Interaction Series.

C. Castelfranchi and R. Falcone. 1998a. Principles of trust for MAS: Cognitive autonomy, social importance, and quantification. In *Proceedings of the International Conference of Multi-Agent Systems (ICMAS'98)*. Paris, France, 72–79.

C. Castelfranchi and R. Falcone. 1998b. Towards a theory of delegation for agent-based systems. *Robotics and Autonomous Systems* 24, 3–4 (Sept. 1998), 141–157.

C. Castelfranchi and R. Falcone. 2000. Trust and control: A dialectic link. *Applied Artificial Intelligence Journal:Special Issue on Trust in Agent, Part I* 14, 8 (2000), 799–823.

C. Castelfranchi and R. Falcone. 2010. *Trust Theory: A Socio-Cognitive and Computational Model*, Michael Wooldridge (Ed.). Series in Agent Technology. Wiley.

C. Castillo, M. Mendoza, and B. Poblete. 2011. Information credibility on Twitter. In *Proceedings of the 20th International Conference on World Wide Web (WWW'11)*. 675–684.

H. Chen, S. Yu, J. Shang, C. Wang, and Z. Ye. 2009. Comparison with several fuzzy trust methods for P2P-based system. In *Proceedings of the International Conference on Information Technology and Computer Science (ITCS'09)*, Vol. 2. Kiev, Ukraine, 188–191.

I. R. Chen, F. Bao, M. J. Chang, and J. H. Cho. 2010. Trust management for encounter-based routing in delay tolerant networks. In *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM'10)*. Miami, Florida, USA, 1–6.

S. H. Chin. 2009. On application of game theory for understanding trust in networks. In *Proceedings of the IEEE International Symposium on Collaborative Technologies and Systems*. Baltimore, MD, 106–110.

J. H. Cho, I. R. Chen, Y. Wang, and K. S. Chan. 2013. Trust-based multi-objective optimization for node-to-task assignment in coalition networks. In *Proceedings of the IEEE International Conference on Parallel and Distributed Systems (ICPADS'13)*. Seoul, Korea, 372–379.

J. H. Cho, A. Swami, and I. R. Chen. 2009. Modeling and analysis of trust management for cognitive mission-driven group communication systems in mobile ad hoc networks. In *Proceedings of the International Conference on Computational Science and Engineering*, Vol. 2. 641–650.

J. H. Cho, A. Swami, and I. R. Chen. 2011. A survey of trust management in mobile ad hoc networks. *IEEE Communications Surveys and Tutorials* 13, 4 (2011), 562–583.

P. Cofta. 2007. The dark side. In *Trust, Complexity and Control: Confidence in a Convergent World*. Wiley, Chichester, UK, 103–117.

J. C. Coleman. 1988. Social capital in the creation of human capital. *American Journal of Sociology* 95 (1988), S95–S120.

A. Corradi, R. Montanari, and D. Tibaldi. 2005. Context-driven adaptation of trust relationships in pervasive collaborative environments. In *Proceedings of the 2005 Symposium on Applications and the Internet Workshops*. Trento, Italy, 178–181.

G. Cvetkovich, M. Siegrist, R. Murray, and S. Tragesser. 2002. New information and social trust: Asymmetry and perseverance of attributions about hazard managers. *Risk Analysis* 22, 2 (April 2002), 359–367.

E. M. Daly and M. Haahr. 2009. Social network analysis for information flow in disconnected delay-tolerant MANETs. *IEEE Transactions on Mobile Computing* 8, 5 (2009), 606–621.

R. Deepa and S. Swamynathan. 2014. A trust model for directory-based service discovery in mobile ad hoc networks. In *Recent Trends in Computer Networks and Distributed Systems Security Communications in Computer and Information Science*, G. Martínez Pérez et al. (Eds.). Vol. 420. Springer-Verlag Berlin Heidelberg, 115–126.

Y. Desmedt, M. Fitzi, and J. B. Nielsen. 2007. Secure protocols with asymmetric trust. In *Proceedings of the 13th International Conference on Theory and Application of Cryptology and Information Security*. Kuching, Malaysia.

J. Dezert and F. Smarandache. 2004. Advances on DSmT. In *Advances and Applications of DSmT for Information Fusion*, Florentin Smarandache and Jean Dezert (Eds.). American Research Press, Rehoboth, NM, USA.

R. Diestel. 2010. *Graph Theory* (4th. ed.). Vol. 173. Springer, Heidelberg. Graduate Texts in Mathematics.

P. A. Dinda. 2004. Addressing the trust asymmetry problem in grid computing with encrypted computation. In *Proceedings of the 7th Workshop on Languages, Compilers, and Run-Time Support for Scalable Systems*. 1–7.

P. Dondio, L. Longo, and S. Barrett. 2008. A translation mechanism for recommendations. In *Trust Management II*, Y. Karabulut, J. Mitchell, P. Hermann, and C. D. Jensen (Eds.). Vol. 263. Springer, Boston, Massachusetts, USA. IFIP International Federation for Information Processing, 87–102.

J. Doyle. 1997. *Rational Decision Making*, R. Wilson and F. Kiel (Eds.). MIT Press, Cambridge, Massachusetts. The MIT Encyclopedia of the Cognitive Sciences.

J. R. Dunn and M. E. Schweitzer. 2005. Feeling and believing: The influence of emotion on trust. *Journal of Personality and Social Psychology* 88, 5 (2005), 736–748.

M. J. Dutta-Bergman. 2004. The impact of completeness and web use motivation on the credibility of e-health information. *Journal of Communication* 54, 2 (2004), 253–269.

M. R. Endsley. 1996. Automation and situation awareness. In *Automation and Human Performance: Theory and Applications - Human Factors in Transportation*, R. Parasuraman and M. Mouloua (Eds.). Lawrence Erlbaum Associates, Inc., Hillsdale, NJ, England.

C. English, S. Terzis, W. Wagealla, H. Lowe, P. Nixon, and A. McGettrick. 2003. Trust dynamics for collaborative global computing. In *Proceedings of the 12th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*. 283–288.

M. Everett and S. P. Borgatti. 2005. Ego network betweenness. *Social Networks* 27, 1 (Jan. 2005), 31–38.

R. Falcone and C. Castelfranchi. 2001. The socio-cognitive dynamics of trust: does trust create trust? In *Lecture Notes in Computer Science*. Springer, London, UK, 55–72. Proceedings of the workshop on Deception, Fraud, and Trust in Agent Societies held during the Autonomous Agents Conference: Trust in Cyber-societies, Integrating the Human and Artificial Perspectives.

X. Fan, S. Oh, M. McNeese, J. Y. H. Cuevas, L. Strater, and M. R. Endsley. 2008. The influence of agent reliability on trust in human-agent collaboration. In *Proceedings of the ACM 15th European Conference on Cognitive Ergonomics: The Ergonomics of Cool Interaction (ECCE'08)*. Madeira, Portugal.

H. Farrell. 2009. Distrust. In *Trust, Distrust, and Power*, R. Hardin (Ed.). Russell Sage Foundation, New York, 84–105.

S. E. Fienberg. 2006. When did Bayesian inference become "Bayesian"? *Bayesian Analysis* 1, 1 (2006), 1–40.

S. Fong and W. Chen. 2010. Social network collaborative filtering framework and online trust factors: A case study on Facebook. In *Proceedings of the 5th International Conference on Digital Information Management*. Thunder Bay, ON, 266–273.

S. Fong, Y. Zhuang, M. Yu, and I. Ma. 2012. Quantitative analysis of trust factors on social network using data mining approach. In *Proceedings of the International Conference on Future Generation Communication Technology*. London, UK, 70–75.

L. C. Freeman. 1977. A set of measures of centrality based on betweenness. *Sociometry* 40, 1 (March 1977), 35–41.

L. C. Freeman. 1979. Centrality in social networks: Conceptual clarification. *Social Networks* 1, 3 (1979), 215–239.

L. C. Freeman, S. P. Borgatti, and D. R. White. 1991. Centrality in valued graphs: A measure of betweenness based on network flow. *Social Networks* 13, 2 (June 1991), 141–154.

D. Gambetta. 1988. Can we trust trust? In *Trust: Making and Breaking Cooperative Relations*, D. Gambetta (Ed.). Basil Blackwell, New York, USA, 213–237.

D. Gillies. 2000. The subjective theory. In *Philosophical Theories of Probability*. Routledge.

K.-I. Goh, E. Oh, B. Kahng, and D. Kim. 2003. Betweenness centrality correlation in social networks. *Physical Review* 67, 1 (2003), 010101:1–010101:4.

J. Golbeck. 2009. Introduction to computing with social trust. In *Computing with Social Trust*, J. Golbeck (Ed.). Springer, London, 1–5. Human-Computer Interaction Series.

N. Griffiths. 2006. A fuzzy approach to reasoning with trust, distrust and insufficient trust. In *Proceedings of the 10th International Workshop on Cooperative Information Agents*. 360–374.

P. Hage and F. Harary. 1995. Eccentricity and centrality in networks. *Social Networks* 17, 1 (Jan. 1995), 57–63.

C. W. Hang and M. P. Singh. 2010. Trust-based recommendation based on graph similarity. In *Proceedings of the 13th Autonomous Agents & Multi-Agent Systems Conference - Workshop on Trust in Agent Societies*. Toronto, Canada.

A. H. Harcourt. 1991. Help, cooperation and trust in animals. In *Cooperation and Prosocial Behaviour*, R. Hinde and J. Groebel (Eds.). Cambridge University Press, 15–26.

R. Hardin. 2002. Trustworthiness. *Trust and Trustworthiness*. Russell Sage Foundation, New York, 28–53.

O. Hasan, L. Brunie, J. M. Pierson, and E. Bertino. 2009. Elimination of subjectivity from trust recommendation. In *2009 IFIP Advances in Information and Communication Technology-Trust Management III*. Vol. 300. Springer, Boston, USA. IFIP International Federation for Information Processing, 65–80.

A. Heddaya and A. Helal. 1996. *Reliability, Availability, Dependability and Performability: A User-Centered View*. Technical Report. Computer Science Department, Boston University.

C. Hewitt. 1991. Open information systems semantics for distributed artificial intelligence. *Artificial Intelligence* 47, 1–3 (1991), 79–106.

B. Hilligoss and S. T. Rieh. 2008. Developing a unifying framework of credibility assessment: Construct, heuristics, and interaction in context. *Information Processing and Management* 44, 4 (2008), 1467–1484.

J. Huang and D. Nicol. 2009. A calculus of trust and its application to PKI and identity management. In *Proceedings of the 8th Symposium on Identity and Trust on the Internet*. 23–37.

T. D. Huynh, N. R. Jennings, and N. R. Shadbolt. 2006. An integrated trust and reputation model for open multi-agent systems. *Autonomous Agents and Multi-Agent Systems* 13, 2 (2006), 119–154.

H. S. James. 2002. The trust paradox: A survey of economic inquiries into the nature of trust and trustworthiness. *Journal of Economic Behavior and Organization* 47, 3 (March 2002), 291–307.

C. Jensen, C. Potts, and C. Jensen. 2005. Privacy practices of internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies* 63, 1–2 (2005), 203–227.

D. Johnson and K. Grayson. 2005. Cognitive and affective trust in service relationships. *Journal of Business Research* 58, 4 (April 2005), 500–507.

B. D. Jones. 1999. Bounded rationality. *Annual Review of Political Science* 2 (1999), 297–321.

A. Jøsang. 1999. An algebra for assessing trust in certification chains. In *Proceedings of the Network and Distributed Systems Security Symposium (NDSS'99)*.

A. Jøsang. 2001. A logic for uncertain probabilities. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 9, 3 (2001), 279–311.

A. Jøsang, E. Gray, and M. Kinateder. 2003. Analyzing topologies of transitive trust. In *Proceedings of the 1st International Workshop on Formal Aspects in Security and Trust*. Pisa, Italy, 9–22.

A. Jøsang and R. Hankin. 2012. Interpretation and fusion of hyper opinions in subjective logic. In *Proceedings of the 15th International Conference on Information Fusion*. Singapore, 1225–1232.

A. Jøsang, R. Hayward, and S. Pope. 2006. Trust network analysis with subjective logic. In *Proceedings of the Australasian Computer Science Conference (ACSC'06)*. Vol. 48, 85–94.

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

A. Jøsang and S. Pope. 2005. Semantic constraints for trust transitivity. In *Proceedings of the 2nd Asia-Pacific Conference of Conceptual Modeling (APCCM'05)*, Vol. 43. 59–68.

A. Jøsang and S. L. Presti. 2004. Analyzing the relationship between risk and trust. In *Proceedings of the 2nd International Conference on Trust Management (iTrust'04)*, Vol. 2995. Springer, 135–145.

L. R. Kalnbach and B. M. Lantz. 1997. *The Effects of Optimism and Willingness to Trust on Work-Related Attitudes and Behaviors: An Application to the Commercial Vehicle Industry*. Technical Report. North Dakota State University.

S. D. Kamvar, M. T. Schlosser, and H. G. Molina. 2003. The eigentrust algorithm for reputation management in P2P networks. In *Proceedings of the 12th International World Wide Web Conference*. Budapest, Hungary, 640–651.

S. Keung and N. Griffiths. 2008. Using recency and relevance to assess trust and reputation. In *Proceedings of the AISB Symposium on Behavior Regulation in Multi-Agent Systems (BRMAS'08)*. Aberdeen, UK.

A. Kittur, B. Suh, and E. H. Chi. 2008. Can you ever trust a wiki?: Impacting perceived trustworthiness in Wikipedia. In *Proceedings of the 2008 ACM Conference on Computer Supported Cooperative Work (CSCW'08)*. San Diego, CA, USA, 477–480.

R. M. Kramer. 1999. Trust and distrust in organizations: Emerging perspectives, enduring questions. *Annual Review of Psychology* 50 (Feb. 1999), 569–598.

A. H. Kydd. 2005. A blind spot of philosophy. *Trust and Mistrust in International Relations*. Princeton University Press.

B. Lahno. 1999. Olli lagerspetz: Trust. The tacit demand. *Ethical Theory and Moral Practice* 2, 4 (1999), 433–435.

G. Q. Lana and C. B. Westphall. 2008. User maturity based trust management for grid computing. In *Proceedings of the 7th International Conference on Networking*. Cancun, Mexico, 758–761.

R. S. Lazarus, J. R. Averill, and E. M. Opton. 1970. Towards a cognitive theory of emotion. In *Feelings and Emotions*, M. B. Arnold (Ed.). Academic Press, New York, 207–232. The Loyola Symposium.

J. D. Lee and N. Moray. 1992. Trust, control strategies and allocation of function in human-machine systems. *Ergonomics* 35, 10 (1992), 1243–1270.

J. D. Lee and K. A. See. 2006. Trust in automation: Designing for appropriate reliance. *Human Factors* 40, 1 (Spring 2006), 50–80.

K. C. Lee and N. Chung. 2009. Understanding factors affecting trust in and satisfaction with mobile banking in Korea: A modified DeLone and McLeans model perspective. *Interacting with Computers* 21, 5–6 (2009), 385–392.

M. Lesani and S. Bagheri. 2006. Fuzzy trust inference in trust graphs and its application in semantic web social networks. In *Proceedings of the World Automation Congress (WAS'06)*. Budapest, Hungary, 1–6.

R. J. Lewicki and B. B. Bunker. 1995. Trust in relationships: A model of development and decline. In *Conflict, Cooperation, and Justice: Essays Inspired by the Work of Morton Deutsch*, Barbara Benedict Bunker and Jeffrey Z. Rubin (Eds.). Jossey-Bass Inc., San Francisco, CA, 133–173. he Jossey-Bass conflict resolution series.

J. David Lewis and A. Weigert. 1985. Trust as a social reality. *Social Forces* 63, 4 (1985), 967–985.

J. Li, R. Li, and J. Kato. 2008. Future trust management framework for mobile Ad Hoc networks. *IEEE Communications Magazine* 46, 4 (April 2008), 108–114. Security in Mobile Ad Hoc and Sensor Networks.

Q. Li, S. Zhu, and G. Cao. 2010. Routing in socially selfish delay tolerant networks. In *Proceedings of the IEEE INFOCOM*. San Diego, CA, 1–9.

Y. Li, M. Chen, Q. Li, and W. Zhang. 2012. Enabling multilevel trust in privacy preserving data mining. *IEEE Transactions on Knowledge and Data Engineering* 24, 9 (2012), 1598–1612.

Z. Liang and W. Shi. 2010. TRECON: A trust-based economic framework for efficient internet routing. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans* 40, 1 (2010), 52–67.

H. Liao, Q. Wang, and G. Li. 2009. A fuzzy logic-based trust model in grid. In *Proceedings of the International Conference on Networks Security, Wireless Communications and Trusted Computing (NSWCTC'09)*. Wuhan, Hubei, China, 608–614.

D. Liben-Nowell and J. Kleinberg. 2003. The link prediction problem for social networks. In *Proceedings of the 12th International Conference on Information and Knowledge Management*. 556–559.

L. Lin and J. Huai. 2009. QGrid: An adaptive trust aware resource management framework. *IEEE Systems Journal* 3, 1 (2009), 78–90.

L.-Y. Lin and C.-Y. Lu. 2010. The influence of corporate image, relationship marketing, and trust on purchase intention: The moderating effects of word-of-mouth. *Tourism Review* 65, 3 (2010), 16–34.

C. Lioma, B. Larsen, H. Schuetze, and P. Ingwersen. 2010. A subjective logic formalisation of the principle of polyrepresentation for information needs. In *Proceedings of the 3rd Symposium on Information Interaction in Context*. 125–134.

N. Luhmann. 1979. *Trust and Power*. John Wiley & Sons Inc.

N. Luhmann. 1990. Familiarity, confidence, trust: problems and alternatives. In *Trust*, D. Gambetta (Ed.). Blackwell.

J. Luo, X. Liu, Y. Zhang, D. Ye, and Z. Xu. 2008. Fuzzy trust recommendation based on collaborative filtering for mobile ad-hoc networks. In *Proceedings of the 33rd IEEE Conference on Local Computer Networks (LCN'08)*. Montreal, Que, 305–311.

S. Ma, J. He, F. Gao, and J. Xu. 2010. A trust quantification algorithm based on fuzzy comprehensive evaluation. In *Proceedings of the International Symposium on Intelligence Information Processing and Trusted Computing (IPTC'10)*. Huanggang, China, 196–199.

G. Mahoney, W. Myrvold, and G. C. Shoja. 2005. Generic reliability trust model. In *Proceedings of Annual Conference on Privacy, Security and Trust*. 113–120.

O. Malacka, J. Samek, and F. Zboril. 2010. Event driven multi-context trust model. In *Proceedings of the 10th International Conference on Intelligent Systems Design and Applications*. Cairo, Egypt, 912–917.

D. W. Manchala. 1998. Trust metrics, models and protocols for electronic commerce transactions. In *Proceedings of the 18th IEEE International Conference on Distributed Computing Systems*. Amsterdam, Netherlands, 312–321.

S. Manna, T. Gedeon, and B. S. U. Mendis. 2010. Enhancement of subjective logic for semantic document analysis using hierarchical document signature. In *Neural Information Processing: Theory and Algorithms*, Vol. 6443. 298–306. The Series Lecture Note in Computer Science.

P. V. Marsden. 2002. Egocentric and sociocentric measures of network centrality. *Social Networks* 24, 4 (Oct. 2002), 407–422.

S. Marsh and P. Briggs. 2009. Examining trust, forgiveness and regret as computational concepts. In *Computing with Social Trust*, J. Golbeck (Ed.). Springer, 9–43. Human-Computer Interaction Series.

S. P. Marsh. 1994. *Formalizing Trust as a Computational Concept*. Ph.D. Dissertation. University of Stirling.

S. P. Marsh and M. R. Dibben. 2005. Trust, untrust, distrust and mistrust: An exploration of the dark(er) side. In *Proceedings of the 3rd International Conference on Trust Management (iTrust'05)*, V. Jennings P. Herrmann, and S. Shiu (Eds.). Vol. 3477. Springer, 17–33. The series Lecture Notes in Computer Science.

I. Matei, J. S. Baras, and T. Jiang. 2009. A composite trust model and its application to collaborative distributed information fusion. In *Proceedings of the 12th International Conference on Information Fusion*. Seattle, WA, 1950–1957.

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

B. McGuinness and A. Leggatt. 2006. Information trust and distrust in a sensemaking task. In *Proceedings of the 11th International Command and Control Research and Technology Symposium*. San Diego, CA.

Merriam and Webster Dictionary. 2015. (2015).

U. F. Minhas, J. Zhang, T. Tran, and R. Cohen. 2010. Intelligent agents in mobile vehicular ad-hoc networks: Leveraging trust modeling based on direct experience with incentives for honesty. In *Proceedings of the 2010 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT'10)*. Toronto, Canada, 243–247.

N. Moray, T. Inagaki, and M. Itoh. 2000. Adaptive automation, trust, and self-confidence in fault management of time-critical tasks. *Journal of Experimental Psychology: Applied* 6, 1 (2000), 44–58.

B. M. Muir. 1994. Trust in automation. Part I. theoretical issues in the study of trust and human intervention in automated systems. *Ergonomics* 37, 11 (1994), 1905–1922.

B. M. Muir and N. Moray. 1996. Trust in automation. Part II. Experimental studies of trust and human intervention in a process control simulation. *Ergonomics* 39, 3 (May 1996), 429–460.

M. Nagy, M. Vargas-Vera, and E. Motta. 2008. Multi agent trust for belief combination on the semantic web. In *Proceedings of the 4th International Conference on Intelligent Computer Communication and Processing*. 261–264.

S. Nefti, F. Meziane, and K. Kasiran. 2005. A fuzzy trust model for e-commerce. In *Proceedings of the 7th IEEE International Conference on E-Commerce Technology*. 401–404.

D. A. Nevell, S. R. Maskell, P. R. Horridge, and H. L. Barnett. 2010. Fusion of data from sources with different levels of trust. In *Proceedings of the 13th Conference on Information Fusion*. 1–7.

M. E. J. Newman. 2001. Clustering and preferential attachment in growing networks. *Physical Review E* 64, 2 (July 2001), 020101:1–020101:4.

M. E. J. Newman. 2005. A measure of betweenness centrality based on random walks. *Social Networks* 27, 1 (Jan. 2005), 39–54.

T. J. Norman and C. Reed. 2010. A logic of delegation. *Artificial Intelligence* 174, 1 (Jan. 2010), 51–71.

N. Oren, T. J. Norman, and A. Preece. 2007. Subjective logic and arguing with evidence. *Artificial Intelligence* 171, 10–15 (July 2007).

R. Parasuraman, T. B. Sheridan, and C. D. Wickens. 2008. Situation awareness, mental workload, and trust in automation: Viable, empirically supported cognitive engineering constructs. *Journal of Cognitive Engineering and Decision Making* 2, 2 (Summer 2008), 140–160.

S. Peng, W. Jia, and G. Wang. 2008. Voting-based clustering algorithm with subjective trust and stability in mobile ad hoc networks. In *Proceedings of the IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*. Shanghai, China, 3–9.

C. Pereitra. 2009. Distrust is not always the complement of trust (Position Paper). *Normative Multi-Agent Systems*, Guido Boella, Pablo Noriega, Gabriella Pigozzi, and Harko Verhagen (Eds.). Dagstuhl, Germany. Dagstuhl Seminar Proceedings.

P. Pong and S. Challa. 2007. Empirical analysis of generalised uncertainty measures with dempster shafer fusion. In *Proceedings of the 10th International Conference on Information Fusion*. Quebec, Que., 1–9.

T. M. Porter. 1995. *Trust in Numbers: The Pursuit of Objectivity in Science and Public Life*. Princeton University Press, UK.

R. D. Putnam. 2000. *Bowling Alone*. Simon and Schuster, New York.

D. Quercia, S. Hailes, and L. Capra. 2006. B-trust: Bayesian trust framework for pervasive computing. In *Proceedings of the 4th International Conference on Trust Management*. Springer, 298–312.

R. J. Rabeloa, L. M. Camarinha-Matos, and H. Afsarmaneshc. 1999. Multi-agent-based agile scheduling. *Robotics and Autonomous Systems, Multi-Agent Systems Applications* 27, 1–2 (April 1999), 15–28.

J. K. Rempel, J. G. Holmes, and M. P. Zanna. 1985. Trust in close relationships. *Journal of Personality and Social Psychology* 49, 1 (July 1985), 95–112.

S. Y. Rieh and D. R. Danielson. 2007. Credibility: A multidisciplinary framework. *Annual Review of Information Science and Technology* 41, 1 (2007), 307–364.

D. M. Romano. 2003. *The Nature of Trust: Conceptual and Operational Clarification*. Ph.D. Dissertation. Department of Psychology, Louisiana State University.

J. B. Rotter. 1980. Interpersonal trust, trustworthiness, and gullibility. *American Psychologist* 35, 1 (Jan. 1980), 1–7.

J. Sabater and C. Sierra. 2002. Reputation and social network analysis in multi-agent systems. In *ACM Proceedings of International Joint Conference on Autonomous Agents and Multiagent Systems*. 475–482.

G. Sabidussi. 1966. The centrality index of a graph. *Psychometrika* 31, 4 (1966), 581–603.

G. Shafer. 1976. *A Mathematical Theory of Evidence*. Princeton University Press, Princeton, NJ.

R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, and Y.-J. Song. 2009. Group-based trust management scheme for clustered wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems* 20, 11 (Nov. 2009), 1698–1712.

C. E. Shannon. 1948. The mathematical theory of communication. *Bell System Technical Journal* 27, 3 (1948), 379–423.

L. Shapley. 1953. A value for n-person games. *Annals of Mathematical Studies* 28 (1953), 307–317.

B. Shelat and F. N. Egger. 2002. What makes people trust online gambling sites? In *ACM Proceedings of Conference on Human Factors in Computing Systems*. 852–853.

D. Shen, G. Chen, K. Pham, and E. Blasch. 2011. A trust-based sensor allocation algorithm in cooperative space search problems. In *Proceedings of SPIE*, Khanh D. Pham, Henry Zmuda, Joseph Lee Cox, and Greg J. Meyer (Eds.), Vol. 8044.

A. Shimbel. 1953. Structural parameters of communication networks. *Bulletin of Mathematical Biophysics* 15, 4 (Dec. 1953), 501–507.

S. Sikdar, S. Adalı, M. Amin, T. Abdelzaher, K. Chan, J. H. Cho, B. Kang, and J. O'Donovan. 2014. Finding true and credible information on twitter. In *Proceedings of the IEEE 17th International Conference on Information Fusion (FUSION)*. Salamanca, Spain, 1–8.

P. Slovic. 1993. Perceived risk, trust, and democracy. *Risk Analysis* 13, 6 (Dec. 1993), 675–682.

P. Smets and R. Kennes. 1994. The transferable belief model. *Artificial Intelligence* 66, 2 (April 1994), 191–234.

B. Solhaug, D. Elgesem, and K. Stolen. 2007. Why trust is not proportional to risk? In *Proceedings of the 2nd International Conference on Availability, Reliability, and Security (ARES'07)*. Vienna, Austria, 11–18.

W. Stallings. 1995. The PGP web of trust. *BYTE* 20, 2 (Feb. 1995), 161–162.

D. Stampouli, M. Brown, and G. Powell. 2010. Fusion of soft information using TBM. In *Proceedings of the 13th Conference on Information Fusion*. Edinburgh, Scotland, 1–8.

A. N. Steinberg, C. L. Bowman, and F. E. White. 1999. Revisions to the JDL data fusion model. In *Proceedings of SPIE (Sensor Fusion: Architectures, Algorithms, and Applications III)*, Vol. 3919. 235–251.

Y. L. Sun, W. Yu, Z. Han, and K. J. R. Liu. 2006. Information theoretic framework of trust modeling and evaluation for ad hoc networks. *Proceedings of the IEEE Journal on Selected Areas in Communications* 24, 2 (Feb. 2006), 305–317.

M. Szomszor, P. Kostkova, and C. St. Louis. 2011. Twitter informatics: Tracking and understanding public reaction during the 2009 Swine Flu Pandemic. In *Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*. Lyon, France, 320–323.

S. Trifunovic, F. Legendre, and C. Anastasiades. 2010. Social trust in opportunistic networks. In *Proceedings of the IEEE INFOCOM Workshop*. San Diego, CA.

R. Trivers. 1971. The evolution of reciprocal altruism. *The Quarterly Review of Biology* 46, 1 (March 1971), 35–57.

R. Trivers. 1985. *Social Evolution*. Benjamin-Cummings Pub Co, Cummings, CA, USA.

P. B. Velloso, R. P. Laufer, D. O. Cunha, O. C. Duarte, and G. Pujolle. 2010. Trust management in mobile ad hoc networks using a scalable maturity-based model. *IEEE Transactions on Network and Service Management* 7, 3 (2010), 172–185.

K. Wang and M. Wu. 2007. A trust approach for node cooperation in MANET. *Mobile Ad-Hoc and Sensor Networks, Lecture Notes in Computer Science* 4864 (2007), 481–491.

Y. Wang, I.-R. Chen, J. H. Cho, K. S. Chan, and A. Swami. 2013. Trust-based service composition and binding for tactical networks with multiple objectives. In *Proceedings of the IEEE MILCOM*. San Diego, CA, 1862–1867.

Y. Wang, Y. C. Lu, I. R. Chen, J. H. Cho, A. Swami, and C. T. Lu. 2014. LogitTrust: A logit regression-based trust model for mobile ad hoc networks. In *Proceedings of the 6th ASE International Conference on Privacy, Security, Risk and Trust (PASSAT'14)*. Cambridge, MA, USA.

Y. Wang and M. Singh. 2010. Evidence-based trust: A mathematical model geared for multiagent systems. *ACM Transactions on Autonomous and Adaptive Systems* 5, 3 (Sept. 2010), 1–25.

Y. Wang and J. Vassileva. 2003. Bayesian network trust model in peer-to-peer networks. In *Proceedings of the 2nd International Workshop Peers and Peer-to-Peer Computing*. Springer, 23–24.

Y. D. Wang and H. H. Emurian. 2005. An overview of online trust: Concepts, elements and implications. *Computers in Human Behavior* 21 (2005), 105–125.

L. Wen, P. Lingdi, W. Chunming, and J. Ming. 2010. Distributed Bayesian network trust model in virtual network. In *Proceedings of the 2nd International Conference on Network Security Wireless Communications and Trusted Computing (NSWCTC'10)*. Wuhan, Hubei, China, 71–74.

Wikipedia. 2015. Definition of Cognition. Retrieved from http://en.wikipedia.org/wiki/Cognition.

Y. Wu, S. Tang, P. Xu, and X.-Y. Li. 2010. Dealing with selfishness and moral hazard in noncooperative wireless networks. *IEEE Transactions on Mobile Computing* 9, 3 (2010), 420–434.

Y. Yamamoto. 1990. A morality based on trust: Some reflections on japanese morality. *Philosophy East and West* 40, 4 (October 1990), 451–469. Understanding Japanese Values.

Z. Yan, P. Zhang, and T. Virtanen. 2003. Trust evaluation based security solutions in ad hoc networks. In *Proceedings of the 7th Nordic Workshop on Security IT Systems (NordSec'03)*. Gjǫdotvik, Norway, 1–10.

Z. Yang, Y. Fan, and B. Zhang. 2010. A fusion model of overall trust relationship from multiple attributes in trusted networks based on dynamic entropy gain. In *Proceedings of the IEEE International Conference on Information Theory and Information Security*. Beijing, China, 323–326.

L. A. Zadeh. 1965. Fuzzy sets. *Information and Control* 8, 3 (June 1965), 338–353.

L. A. Zadeh. 1983. The role of fuzzy logic in the management of uncertainty in expert systems. *Fuzzy Sets and Systems* 11, 1–3 (March 1983), 197–198.

J. Zhang, A. A. Ghorbani, and R. Cohen. 2006. An improved familiarity measurement for formalization of trust in e-commerce based multi-agent systems. In *Proceedings of 2006 International Conference on Privacy, Security, and Trust: Bridge the Gap Between PST Technologies and Business Services*.

Y. Zheng, R. Kantola, and P. Zhang. 2011. A research model for human-computer trust interaction. In *Proceedings of the IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'11)*. Changsha, China, 274–281.

C.-N. Zieglera and J. Golbeck. 2007. Investigating interactions of trust and interest similarity. *Decision Support Systems* 43, 2 (March 2007), 460–475. Emerging Issues in Collaborative Commerce.

C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas. 2005. Quantitative trust establishment framework for reliable data packet delivery in MANETs. In *Proceedings of the 3rd ACM Workshop on Security for Ad Hoc and Sensor Networks*. Alexandria, VA, 1–10.

Received January 2014; revised July 2015; accepted August 2015