

# Trust Networks: Interpersonal, Sensor, and Social

Krishnaprasad Thirunarayan and Pramod Anantharam

*Ohio Center of Excellence in Knowledge-enabled Computing - Kno.e.sis*

*Wright State University, Dayton, OH-45435*

[t.k.prasad@wright.edu](mailto:t.k.prasad@wright.edu), [pramod@knoesis.org](mailto:pramod@knoesis.org)

## ABSTRACT

*Trust relationships occur naturally in many diverse contexts such as ecommerce, interpersonal interactions, social networks, sensor web, etc. As agents providing content and services become increasingly removed from the agents that consume them, the issue of robust trust inference and update become critical. Unfortunately, there is neither a universal notion of trust that is applicable to all domains nor a clear explication of its semantics or computation in many situations. In this beginner's level tutorial, we motivate the trust problem, explain the relevant concepts, summarize research in modeling trust and gleaning trustworthiness, and discuss challenges confronting us in this process.*

**KEYWORDS:** trust vs. reputation, trust ontology, gleaning trustworthiness, beta-PDF, trust metrics (propagation: chaining and aggregation), social and sensor networks, security attacks.

## 1. INTRODUCTION

Trust relationships occur naturally in many diverse contexts such as ecommerce, social interactions, (semantic) social networks, ad hoc mobile networks, distributed systems, decision-support systems, (semantic) sensor web, etc. As the connections and interactions between humans and/or machines (collectively called agents) evolve, and as the agents providing content and services become increasingly removed from the agents that consume them, and as miscreants attempt to corrupt, subvert or attack existing infrastructure, the issue of robust trust inference (e.g., gleaning, aggregation, propagation) and update (collectively called trust management) become critical. Unfortunately, there is neither a universal notion of trust that is applicable to all domains nor a clear explication of its semantics or computation in many situations. Furthermore, because

Web, social networking and sensor information often provide complementary and overlapping information about an activity or event that are critical for overall situational awareness, there is a unique need for developing an understanding of and techniques for managing trust that span all these information channels.

This paper is organized as follows: In Section 2, we provide examples to motivate the trust problem. In Section 3, we elucidate characteristics of trust and explain related concepts. In Section 4, we discuss our trust ontology. In Section 5, we summarize trust research by showing illustrative examples of how to glean trustworthiness. In Section 6, we discuss some of the challenges confronting us going forward in the realm of interpersonal, sensor and social networks.

## 2. MOTIVATION

We present real-life examples to underscore the fundamental nature of trust problem.

### 2.1. Interpersonal Networks

- *With which neighbor should we leave our children over the weekend when we are required to be at the hospital?*
- *Who should be named as a guardian for our children in the Will?*

Note that (i) there is uncertainty and incompleteness in our knowledge about the unraveling situation, (ii) there is not only an expectation of good outcome but also concern about bad outcome, and (iii) there is a need for immediate action. Furthermore, the threshold for trust in the second case is significantly higher than the threshold for the first case.

### 2.2. Social Networks

–**SUBJECT:** [TitanPad] Amit Sheth invited you to an EtherPad document.

–**CONTENT:** View it here:

<http://knoesis.titanpad.com/200>

I received the above email from a collaborator. Is this a genuine request or a trap, especially given that in the past we have collaborated using only Google Docs, and TitanPad was unfamiliar to me, and there may be a need to act immediately to edit the shared document? Similarly, one always has a nagging feeling about clicking on a <http://bit.ly-URL>, or about relying on a product review (when only a few reviews are present).

### 2.3. Sensor Networks

*Given a weather sensor network-based prediction of a potential tornado in the vicinity of a city, should we mobilize emergency response teams ahead of time?*

*When our van's TCS (Traction Control System) indicator light comes on intermittently, is the indicator light faulty or the traction control system? Similarly, when our van's Check Engine light comes on, is indicator light faulty or the transmission?*

In fact, in our van's case, the TCS indicator light and the transmission were faulty.

### 2.4. Common Issues Related to Trust

In all the above examples, we have a *Trustor* who must choose whether and how much to trust a *Trustee*, an *Action* by which the trustor is choosing to be vulnerable to the trustee based on an assessment of trustee's nature, and a *Context* in which the potential negative consequences of betrayal outweigh any perceived positive results [12].

There are two sides to trust management: Trustor assesses trustee for dependability in a given context and then decides to act accordingly. On the other hand, trustee tries to come across in positive light about its suitability, reliability and quality of service.

In general, we track trust: (i) to predict future behavior; (ii) to incentivize "good" behavior and discourage "bad" behavior; and (iii) to detect malicious entities.

## 3. TRUST-RELATED CONCEPTS

### 3.1. Trust Definitions

(Psychology slant) *Trust* in a person is a commitment to an action based on a belief that the future actions of that person will lead to good outcome [10].

(Probability slant) *Trust* (or, symmetrically, distrust) is a level of subjective probability with which an agent assesses that another agent will perform a particular action, both before and independently of such an action being monitored [15].

### 3.2. Trustworthiness Definition

(Psychology Slant) *Trustworthiness* is a collection of qualities of an agent that leads them to be considered as deserving of trust from others (in one or more environments, under different conditions, and to different degrees) [12].

(Probability slant) *Trustworthiness* is the objective probability that the trustee performs a particular action on which the interests of the trustor depend.

### 3.3. Trust versus Trustworthiness

*Trust disposition depends on potentially quantified trustworthiness qualities and context-based trust threshold.* For example, in the context of trusting strangers, people in the West will trust for lower levels of trustworthiness than people in the Gulf [1].

Trustworthy system produces expected behavior and is not susceptible to subversion. In other words, trustworthiness is the assurance that a system will perform as expected despite environmental disruptions, human and operator errors, hostile attacks, and implementation errors.

### 3.4. Reputation versus Trust

(Community-based) *reputation* is the community or public estimation of standing for merit, achievement, reliability, etc<sup>1</sup>. Alternatively, *reputation* is the opinion (or a social evaluation) of a community toward a person, a group of people, or an organization on a certain criterion<sup>2</sup>. (Cf., Brand-value, PageRank [16], eBay profile, etc.)

Reputation can be a basis for trust. However, they are different notions, as illustrated by Josang.

*I trust you because of your good reputation.  
I trust you despite your bad reputation.  
Do you still trust Toyota brand?*

<sup>1</sup> Dictionary.com

<sup>2</sup> Wikipedia.com

Trust is local and subjective; reputation is global and objective. Security refers to resistance to attacks.

Reputation is overloaded in that community-based reputation differs from temporal reputation-based process. The latter elicits trust for sustained good behavior over time.

Trust is a relationship among agents. In contrast, belief is a relationship between an agent and a statement.

#### 4. TRUST ONTOLOGY

Consider the following fragment of English involving trust information, and its abstract representation shown in Figure 1 [2].

- Alice trusts Bob for recommending good car mechanic.
- Bob trusts Dick to be a good car mechanic.
- Charlie does not trust Dick to be a good car mechanic.
- Alice trusts Bob more than Charlie, for recommending good car mechanic.
- Alice trusts Charlie more than Bob, for recommending good baby sitter.

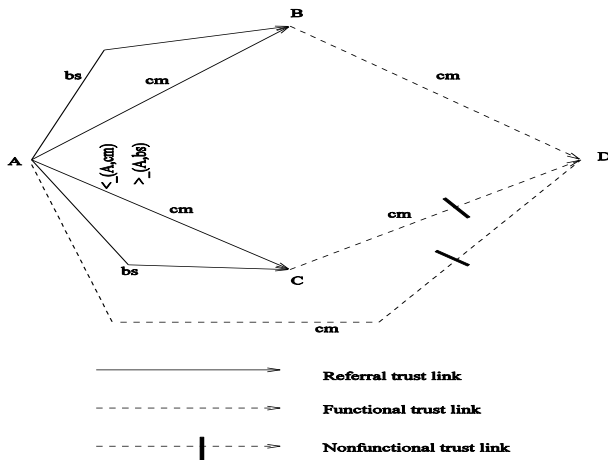


Figure 1: Example Trust Network

A *trust network* is a node-labeled, edge-labeled, in-arc ordered, directed graph data structure. The *semantics of trust* is captured by specifying the meaning of the trust network in terms of how “network elements” relate to or compose with each other using logic, probability theory, statistics, or path constraints. *Inference algorithms* are efficient graph-based procedures for querying or determining trust values.

In order to better understand trust concepts and relate various approaches to trust in the literature, we developed

a simple ontology of trust. See Figures 2 and 3 for details. Trust relationship is 6-tuple: (*trustor*, *trust type*, *trust value*, *trust scope*, *trust process*, *trustee*), where, *trust type* represents the nature of trust relationship, *trust value* quantifies trustworthiness for comparison, *trust scope* represents applicable context for trust, and *trust process* represents the method by which the trust value is created and maintained.

##### Trust Type:

- *Referral Trust* (trust in belief) – Agent a1 trusts agent a2’s ability to recommend another agent.
- *(Non-)Functional Trust* (trust in performance) – Agent a1 (dis)trusts agent a2’s ability to perform an action.

Trust Value: E.g., Star rating, numeric rating, or partial ordering.

Trust Scope: E.g., Car mechanic, identity, service, etc.

##### Trust Process:

- Primitive (for functional and referral links)
  - *(Temporal) Reputation* – based on past behavior.
  - *Policy* – based on explicitly stated constraints.
  - *Evidence* – based on seeking/verifying evidence.
  - *Provenance* – based on lineage information.
- Composite (for admissible paths)
  - Via propagation (chaining and aggregation)

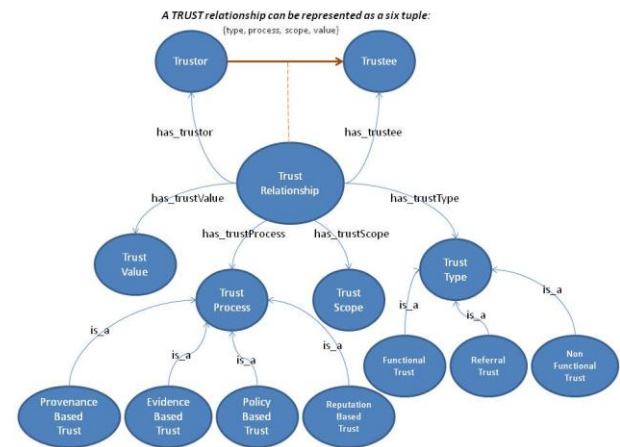


Figure 2: Trust Ontology

To provide a unified illustration of the trust processes consider hiring of a Search Engineer. (Temporal) Reputation-based process is exemplified by use of past job experience. Policy-based process can use scores on screening tests. Evidence-based process uses multiple interviews (phone, on-site, R&D team) for assessing the

candidate's merits. Provenance-based process considers University of graduation.

Example Trust Network illustrating Ontology Concepts

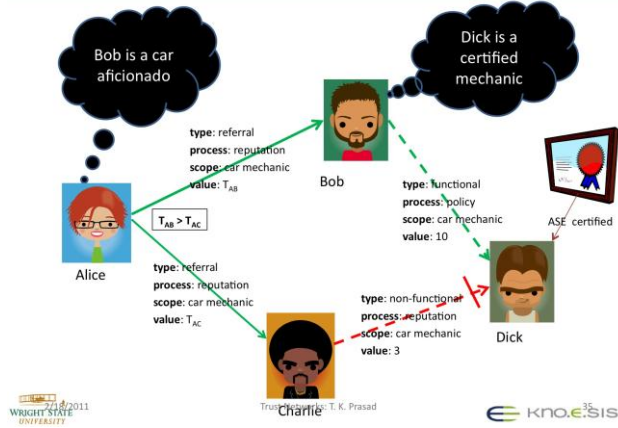


Figure 3: Example illustrating trust ontology

5. GLEANING TRUSTWORTHINESS: PRACTICAL EXAMPLES

We now illustrate how one can glean trustworthiness in different contexts.

5.1 Direct Trust: Functional Trust and Reputation-based Process

Direct trust can be inferred using a large number of observations made in two orthogonal ways: *over a period of time* or *by several agents*. Quantitative values for referral and functional trust in mobile *ad-hoc* networks and sensor networks can be obtained using temporal reputation-based process. Both qualitative and quantitative information for referral and functional trust in product rating systems can be obtained using community reputation-based process. We now motivate and discuss the details of an approach to formalizing reputation-based process that is in wide use.

5.1.1. Desiderata for Trustworthiness Computation Function

- Initialization Problem:* How do we get initial trust value?
- Update Problem:* How do we reflect the observed behavior in the current value dynamically?
- Trusting Trust Issue:* How do we mirror uncertainty in our estimates as a function of observations?
- Efficiency Problem:* How do we store and update values efficiently?

5.1.2. Beta Distribution

Beta-PDF provides a satisfactory mathematical foundation for reputation-based systems. Let  $x$  be the probability for a binary event. If the prior distribution of  $x$  is uniform, then the beta distribution gives posterior distribution of  $x$  after observing  $\alpha - 1$  occurrences of event with probability  $x$  and  $\beta - 1$  occurrences of the complementary event with probability  $(1-x)$ .

$$f(x; \alpha, \beta) = \frac{x^{\alpha-1}(1-x)^{\beta-1}}{\int_0^1 u^{\alpha-1}(1-u)^{\beta-1} du}$$

$$= \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1}(1-x)^{\beta-1}$$

$$= \frac{1}{B(\alpha, \beta)} x^{\alpha-1}(1-x)^{\beta-1}$$

$$E(X) = \frac{\alpha}{\alpha + \beta}$$

$$E(X^2) = \frac{\alpha(\alpha + 1)}{(\alpha + \beta)(\alpha + \beta + 1)}$$

$$Var(X) = \frac{\alpha\beta}{(\alpha + \beta)^2(\alpha + \beta + 1)}$$

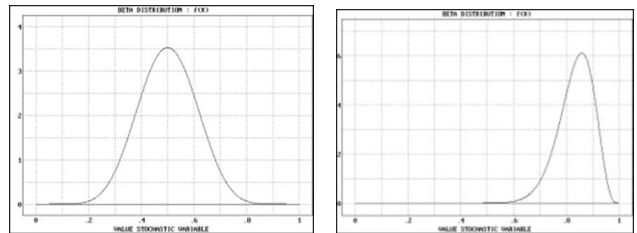


Figure 4: Beta-PDF(alpha=10;beta=10) and Beta-PDF(alpha=25,beta=5)

Specifically, let a (potentially unfair) coin have probability  $x$  of coming up with heads, and probability  $(1-x)$  of coming up with tail. Suppose we perform  $(r + s)$  coin tosses and the coin turns up with heads  $r$  times and with tails  $s$  times. Then the beta-distribution [4] with parameters  $(r+1, s+1)$  provides the best estimate of the distribution of the probability  $x$  given these observations.

Dynamic trustworthiness of a sensor or a vendor can be characterized using beta probability distribution function Beta-PDF( $\alpha, \beta$ ) gleaned from total number of correct (supportive)  $r = (\alpha - 1)$  and total number of erroneous (opposing)  $s = (\beta - 1)$  observations so far, and the overall trustworthiness (reputation) can be equated to its mean:

$\alpha/\alpha + \beta$ . The beta-PDF is intuitively satisfactory, mathematically precise, and computationally tractable. Specifically, it addresses all our requirements as follows:

*Initialization Problem:* It assumes that all probability values are equally likely.

*Update Problem:* It updates  $(\alpha, \beta)$  by incrementing  $\alpha$  for every correct (supportive) observation and  $\beta$  for every erroneous (opposing) observation.

*Trusting Trust Issue:* The graph peaks at the mean and the variance diminishes with the number of observations.

*Efficiency Problem:* It stores/updates only two numbers.

### 5.1.3. Information Theoretic Interpretation of Trustworthiness Probability

Intuitively, probability values of 0 and 1 imply certainty, while probability value of 0.5 implies absolute uncertainty. This can be formalized by mapping probability value in  $[0, 1]$  to trust value in  $[-1, 1]$ , using information theory.

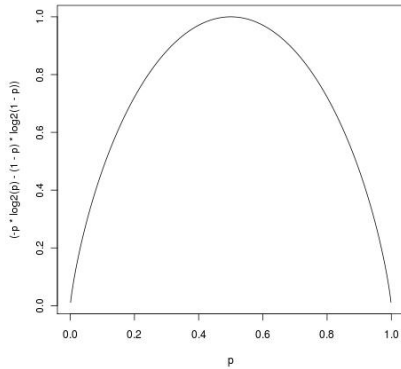


Figure 5: Uncertainty as a function of probability

## 5.2. Direct Trust: Functional Trust and Policy-based Process

A general approach to trust assessment uses (i) domain dependent qualities for determining trustworthiness based on content (data) and on external cues (metadata), and (ii) domain independent mapping to trust values or levels through quantification and classification [17].

For example, trustworthiness of Wikipedia articles can be assessed based on domain dependent content-based quality factors such as references to peer-reviewed publications, proportion of paragraphs with citation, article size, etc., and metadata-based credibility factors such as author connectivity, edit pattern and development history, revision count, proportion of reverted edits including normal and due to vandalism, mean time between edits, mean edit length, etc. Trustworthiness can

be quantified in a domain independent way using dispersion degree score that captures the extent of deviation from the mean. For evaluation metric, normalized discounted cumulative gain (NDCG) can be used to compare ranking based on trust levels (determined from trustworthiness scores) to gold standard classification.

Another example is the estimation of a website’s trustworthiness based on the criticality of data exchanged with it. Specifically, each of the following pieces of information carries with it different level of sensitivity: email address, username and password, phone number, home address, date of birth, social security number, etc. Intuitively, a piece of data is critical if it is exchanged with a small number of highly trusted sites [18].

## 5.3. Indirect Trust: Referral and Functional Trust using a Variety of Trust Metrics

Trust between a pair of users can be gleaned on the basis of their similarity, where similarity can be quantified in a number of ways such as using average difference in ratings, overall correlation of ratings, correlation on extremes, etc. [19]. In fact, collaborative filtering uses similarity measures (such as profile-based, item-ratings based, item-category based) between a user and other users to predict item-ratings by the user. This approach is items-agnostic and scales well over time with large number of items. However, it suffers from (i) *data sparsity problem* when small number of items are common between users, (ii) *cold start user problem*, when a user has rated only a small number of items, and (iii) is prone to *copy-profile attack* where an attacker can create a targeted-user-like profile to manipulate recommendations.

Trust-aware Recommender Systems (TaRS) use explicit/direct trust between users to predict implicit/indirect trust between users through chaining [20]. They overcome limitations of collaborative filtering because trust propagation improves coverage, a single trust link from a new user can enable the user to inherit several “parental” recommendations, and fake identities are not trusted by an active user.

### 5.3.1. Trust Propagation Frameworks

There are a host of approaches in the literature that present *trust management frameworks* and formalize *trust propagation*, that is, *chaining* of trust edges into paths, *aggregation* of trust from multiple sources, and *overriding* [2,5,6,8,9,10,21,22,23]. In the absence of an objective, direct semantics of trust, it is very difficult to evaluate various approaches to trust for validity. This is made

worse by the lack of concrete, transparent examples of trust computations that show all the consequences of a specified approach. In a number of situations, it is in fact possible to reverse engineer framework parameters to reflect any desirable semantics of a trust network, making the comparison of frameworks so much harder.

### 5.3.2. Trust Propagation Algorithms

Broadly speaking, trust propagation algorithms work on DAGs extracted from potentially cyclic trust networks and fall into two categories: top-down and bottom-up. In *top-down* approach, trust value for a source in a target is predicted by aggregating trust values in the target inherited from source's "trusted" parents weighted with trust value in the corresponding parent [24]. In *bottom-up* approach, trust value for a source in a target is predicted by aggregating trust scores in target inherited from target's "trusted" neighbors weighted with trust value in the corresponding neighbor [21]. For instance, the two approaches cited above interpret Figure 6(a) similarly with q trusting s. On the other hand, they interpret Figure 6(b) differently with the top-down approach being ambiguous about q trusting s, while the bottom-up approach concludes that q distrusts s.



(a) Same Interpretation (b) Different Interpretation  
Figure 6: Comparative analysis example: top-down vs. bottom-up

Figure 7 illustrates the TidalTrust algorithm where the trust computation is top-down and using weighted averages. Specifically,  $T(E, Sink) = T(C, Sink) = 2$ ,  $T(B, Sink) = (3*2+6*5)/(3+6) = 4$ , and  $T(Source, Sink) = (4*4+2*7)/(4+2) = 5$ .

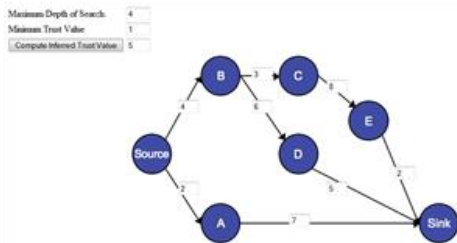


Figure 7: TidalTrust Trust Computation Example

Figure 8 shows a well-founded cyclic trust network and binary trust conclusions.

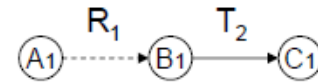


Figure 8: Cyclic Trust Network

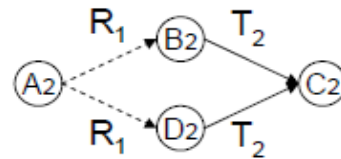
### 5.3.3. Trust Propagation Rules: Axioms for Trust Models

Sun et al [5] describes an interesting approach to trust computation in ad-hoc mobile networks by first providing an axiomatic basis for trust models as shown below and then providing concrete rules for combining trust values.

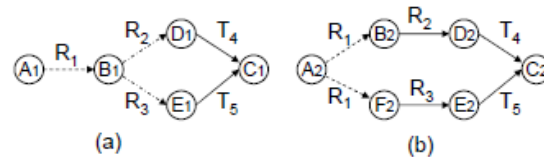
**Rule 1:** Concatenation propagation does not increase trust. For example, to satisfy Rule 1, one can use  $T(A_1, C_1) = R_1 * T_2$  if  $R_1 > 0$  and  $T_2 > 0$ .



**Rule 2:** Multipath propagation does not reduce trust. For example, to satisfy Rule 2, one can combine the trust values on the two paths as  $T(A_2, C_2) = (R1(R1*T2) + R1(R1*T2)) / (R1 + R1)$ , where the italicized values refer to the upper path and boldface values refer to the lower path in case one wants to consider different trust values.



**Rule 3:** Trust based on multiple referrals from a single source should not be higher than that from independent sources. That is,  $T(A_1, C_1) \leq T(A_2, C_2)$ .



Beta-reputation system [7] chains opinions o1 and o2 to obtain discounted opinion (each with three components [belief b, disbelief d, uncertainty u]) as  $b = b1 * b2$ ,  $d = b1 * d2$ , and  $u = d1 + u1 + b1 * u2$ .

## 6. RESEARCH CHALLENGES

In general, practical trustworthiness assessment involves

- Finding online substitutes for traditional cues to derive measures of trust.
- Creating efficient and secure systems for managing and deriving trust, to support decision-making.

### 6.1. Sensor Networks

We have proposed an iterative approach to abstracting low-level numeric observations (e.g., color, shape, etc.) to high-level human comprehensible perceptions (e.g., apple) to obtain actionable situation awareness using background knowledge (codified in the form of bipartite graph connecting low-level observations to high-level percepts) [25]. Specifically, background knowledge and the current observations are used to determine best possible quality to observe (called focus) so as to come up with most specific perception that can account for all the observations. In fact, our formalization of perception cycle identifies it as an instance of abductive reasoning (reasoning to best explanation) that is used extensively in areas such as medical diagnosis [25]. Now, we have extended this work further by lifting trustworthiness of observations to that of sensors and perceptions.

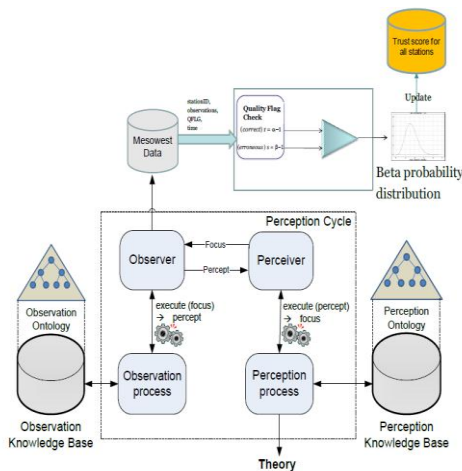


Figure 9: Trusted Perception Cycle

We have developed an application based on Weather Ontology that takes weather phenomena values from the Mesowest<sup>3</sup> Weather Dataset for ~800 stations collected for a blizzard during 4/1-6/03 and maps it to the corresponding weather features using rules defined by

<sup>3</sup> <http://mesowest.utah.edu/index.html>

NOAA (National Oceanic and Atmospheric Administration). We used quality flags (OK, CAUTION, SUSPECT) associated with observations from a sensor station over time to derive reputation of a sensor by applying beta-PDF and trustworthiness of a perceptual theory that explains the observation.

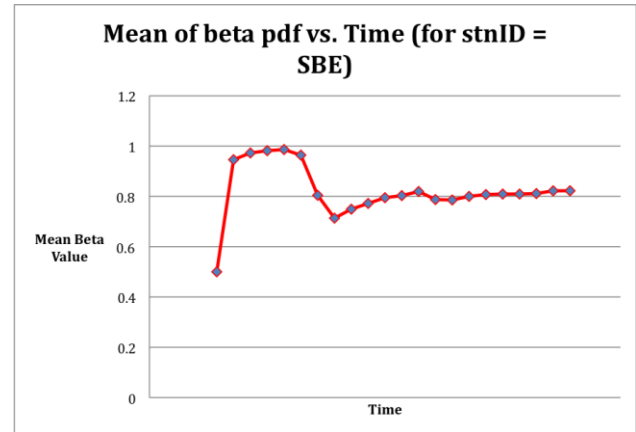


Figure 10: Sensor trustworthiness as a function of time

The demo located at [14] is a visualization of the perception cycle, and the trust computation and update.

Going forward, salient research issues to be addressed include:

- Outlier detection algorithms
  - For homogeneous networks based on statistical techniques
  - For heterogeneous networks (sensor + social) based on domain models
- Distinguishing between abnormal phenomenon (observation), malfunction (of a sensor), and compromised behavior (of a sensor). That is, characterizing abnormal situations faulty behaviors, and malicious attacks.

Ganeriwal et al [11] describe a reputation-based framework for sensor networks based on beta-PDF and explain how it is secure with respect to bad mouthing and ballot stuffing attacks.

### 6.2. Social Networks

Our research in social networks has focused on:

- Studying semantic issues relevant to trust.
- Developing models of trust/trust metrics to formalize indirect trust.

Traditionally, trust between a pair of users is modeled as a real number in [0,1] or [-1,1]. This facilitates trust computation but is too fine-grained and imposes a total

order. Furthermore, there are inherent difficulties in acquiring and justifying computed trust values. As stated by Guha et al [6]: While continuous-valued trusts are mathematically clean, from the standpoint of usability, most real-world systems will in fact use discrete values at which one user can rate another. Users often rate other users (e.g. vendors, reviewers) or contribution of other users (e.g. reviews) using discrete values like star ratings. Epinions, provides a qualitative way of adding other users to a trust circle. Epinions, Ebay, Amazon, Facebook, etc. all use small sets for (dis)trust/rating values.

We formalized trust in terms of partial orders (with emphasis on relative magnitude) in such a way that our semantics is local (that is, semantics of a node is dependent on the semantics of its neighboring nodes and the topology of the immediate network neighborhood) but realistic, distinguishes functional and referral trust, distinguishes direct and inferred trust, and enables direct trust to override conflicting inferred trust, representing ambiguity and trust scopes explicitly. Our local approach, described in [2], has limitations because it does not explicitly address trust discounting as a function of the trust path length but the framework can be adapted to account for it.

In the context of product rating networks, there are several practical issues that can be addressed to improve interpretation of the ratings. Numeric ratings can be refined using text reviews by separate ratings of vendor or about extraneous features of a product from ratings of product proper. For instance, many reviews deal with Amazon's sale and return policies. The book "The Goldilock's Enigma" by Paul Davies' got bad reviews because it was also published under the title "Cosmic Jackpot" in U.K., which the customers felt conveyed that it was a different book. One can check consistency between rating and review using sentiment analysis to amplify hidden sentiments or correct misrepresentations. For instance, a phone was rated as 1-star because it was the best according to the reviewer! In general, trustworthiness of a product should be based on quantitative summaries such as star ratings and qualitative reviews that reflect sentiments about product quality, content that reflects reviewer expertise, and feedback on the reviews. Note that most of these networks involve chaining of just one referral and one (non-)functional link.

Going forward, salient research issues to be addressed include:

- Determination of trust / influence from social networks
  - Using text analytics on communication.
  - Analysis of network topology, e.g., follower relationship, friend relationship, etc.

- Determination of untrustworthy and anti-social elements in social networks
- Determination of relative trust in social networks, for conflict-resolution, preferential filtering, etc.
- Evolving trust ontology
- Introducing trust threshold for binary decision to act in spite of vulnerability/risk
- Structuring trust scope using class hierarchy
- Structuring trust values
- Refining trust types and scopes
- Developing direct semantics for trust propagation
- Improving security, especially by exploiting different trust processes to detect attacks and be robust with respect to bad mouthing attack, ballot stuffing attack, sleeper attack (using temporal trust discounting proportional to trust value, and policy to ward-off attack due to reputation), Sybil attack, newcomer attack, etc.
- Intelligent integration of mobile sensor and social data for situational awareness
  - To exploit complementary and corroborative evidence provided by them
  - To obtain qualitative and quantitative context
  - To improve robustness and completeness to incorporate socio-cultural, linguistic and behavioral knowledge as part of ontologies to improve semantic processing and analysis of data.

### 6.3. Interpersonal Networks

Going forward, salient research issues to be addressed include:

- Determining linguistic clues that betray trustworthiness.
- Designing experiments for gauging interpersonal trust in real world situations, especially by developing techniques and tools to detect and amplify useful signals that more accurately predict trust and trustworthiness
- Study cross-cultural differences in trustworthiness qualities and trust thresholds to better understand what aspects improve *influence* and what aspects flag *manipulation*?

## 7. CONCLUSIONS

In this tutorial, we have provided simple examples to motivate practical trust issues, explained salient features that characterize trust and distinguishes it from related concepts such as trustworthiness, reputation, security, belief, etc. We also discussed our trust ontology, our research accomplishments, and showed illustrative examples of gleaning trustworthiness. Finally, we touched upon some research challenges for modeling trust and gleaning trustworthiness in the context of interpersonal, sensor and social networks.

## ACKNOWLEDGEMENTS

The authors would like to thank Cory Henson and Professor Amit Sheth for valuable discussions that shaped our thoughts and made this introductory tutorial presentation more accessible to general audience.

## REFERENCES

- [1] I. Bohnet, B. Herrmann, and R. Zeckhauser, "Trust and the Reference points for Trustworthiness in Gulf and Western Countries," Vol. 125, No. 2, pp. 811-828, May 2010.
- [2] K. Thirunarayan, D. K. Althuru, C. A. Henson, and A. P. Sheth, "A Local Qualitative Approach to Referral and Functional Trust," The 4th Indian International Conference on Artificial Intelligence (IICAI-09), pp. 574-588, December 2009.
- [3] P. Anantharam, C. A. Henson, K. Thirunarayan, and A. P. Sheth, "Trust Model for Semantic Sensor and Social Networks: A Preliminary Report," National Aerospace & Electronics Conference (NAECON), Dayton Ohio, July 14-16, 2010.
- [4] "Beta distribution," Wikipedia [website], Available: [http://en.wikipedia.org/wiki/Beta\\_distribution](http://en.wikipedia.org/wiki/Beta_distribution).
- [5] Y. L. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," IEEE Journal on Selected Areas in Communications, Vol. 24, Issue 2, pp. 305-316, February 2006.
- [6] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins, "Propagation of trust and distrust," The 13th international Conference on World Wide Web (WWW '04), pp. 403-412, 2004.
- [7] A. Jøsang and R. Ismail, "The Beta Reputation System," The 15<sup>th</sup> Bled Electronic Commerce Conference, Bled, Slovenia, June 2002.
- [8] M. Richardson, R. Agrawal and P. Domingos, "Trust Management for the Semantic Web," The Second International Semantic Web Conference, pp. 351-368, 2003.
- [9] P. Massa, and P. Avesani, "Controversial users demand local trust metrics: an experimental study on epinions.com community," The 25th American Association for Artificial Intelligence Conference, pp. 121-126, 2005.
- [10] J. Golbeck and J. Hendler, "Inferring binary trust relationships in Web-based social networks," ACM Transactions on Internet Technology, Vol. 6, No. 4, pp. 497-529, 2006.
- [11] S. Ganeriwala, L. Balzano, and M. B. Srivastava, "Reputation-based Framework for High Integrity Sensor Networks," ACM Transactions on Sensor Networks (TOSN), Vol. 4, Issue. 3, pp. 1-37, June 2008.
- [12] A. Russell, "TRUST Proposers' Day Briefing IARPA-BAA-10-03 Overview," IARPA.
- [13] J. Golbeck and B. Parsia, "Trust Network-Based Filtering of Aggregated Claims," International Journal of Metadata, Semantics and Ontologies, Vol. 1, No. 1, pp. 58-65, 2006.
- [14] "Trusted Perception Cycle" [Demo], Available: <http://www.youtube.com/watch?v=ITxzghCjGgU>
- [15] D. Gambetta, "Can We Trust Trust?," In Trust: Making and Breaking Cooperative Relations (1988).
- [16] S. Brin and L. Page, "The Anatomy of a Large-Scale Hypertextual Web Search Engine," Computer Networks, Vol. 30, No. (1-7), pp. 107-117, 1998.
- [17] S. T. Moturu and H. Liu, "Evaluating the trustworthiness of Wikipedia articles through quality and credibility," Int. Sym. Wikis, 2009.
- [18] M. d'Aquin, S. Elahi, and E. Motta, "Semantic monitoring of personal web activity to support the management of trust and privacy," SPOT 2010: 2nd Workshop on Trust and Privacy on the Social and Semantic Web, Heraklion, Greece, May 31, 2010,
- [19] U. Kuter and J. Golbeck, "Semantic Web Service Composition in Social Environments," 8th International Semantic Web Conference, ISWC 2009, Vol. 5823, pp. 344-358, Chantilly, VA, USA, October 25-29, 2009.
- [20] P. Massa and P. Avesani, "Trust-aware recommender systems," ACM Conference on Recommender Systems (RecSys, 2007), pp. 17-24, 2007.
- [21] V. G. Bintzios, T. G. Papaioannou, and G. D. Stamoulis, "An Effective Approach for Accurate Estimation of Trust of Distant Information Sources in the Semantic Web," Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2006), pp. 69-74, Lyon, France, June 2006.
- [22] A. Jøsang. "Fission of Opinions in Subjective Logic," The 12th International Conference on Information Fusion (FUSION 2009), Seattle, July 2009.
- [23] U. Kuter and J. Golbeck, "SUNNY: A New Algorithm for Trust Inference in Social Networks Using Probabilistic Confidence Models," The Twenty-Second AAAI Conference on Artificial Intelligence, pp. 1377-1382, Vancouver, British Columbia, Canada, July 22-26, 2007.
- [24] K. Thirunarayan and R. Verma. "A Framework for Trust and Distrust Networks," Web 2.0 Trust Workshop (W2Trust), June 2008.
- [25] "Ontology of Perception," Available: [http://wiki.knoesis.org/index.php/Ontology\\_of\\_Perception](http://wiki.knoesis.org/index.php/Ontology_of_Perception)