

Predicting Trust Relations Within a Social Network: A Case Study on Emergency Response

Nikhita Vedula

Department of Computer Science and
Engineering
Ohio State University
vedula.5@osu.edu

Srinivasan Parthasarathy

Department of Computer Science and
Engineering
Ohio State University
srini@cse.ohio-state.edu

Valerie L. Shalin

Department of Psychology and
Kno.e.sis
Wright State University
valerie@knoesis.org

ABSTRACT

Trust is a fundamental construct underpinning modern society and the social exchanges it contains. The rise of Web 2.0 technologies and the increased use of online social networks, promotes the study of trust among users. Drawing on social and psychological theory, we detect pairwise and global trust relations between users in the context of emergent real-world crisis scenarios. In such situations and scale, seeking explicit pairwise trust assessments between users is impractical. Instead, in an unsupervised manner we integrate the implicit factors of social influence exerted by each user over the network, the underlying network structural topology and the affective valence expressed by the users in the textual content they communicate. A key finding is the importance of modeling influence and affective valence in such exchanges and their role in detecting stable trust relationships. We extensively evaluate these ideas and demonstrate significant gains over competitive baselines across multiple datasets drawn from both crisis and non-crisis scenarios, including those with normative ground truth.

ACM Reference format:

Nikhita Vedula, Srinivasan Parthasarathy, and Valerie L. Shalin. 2017. Predicting Trust Relations Within a Social Network: A Case Study on Emergency Response. In *Proceedings of WebSci '17, Troy, NY, USA, June 25-28, 2017*, 10 pages.
<https://doi.org/http://dx.doi.org/10.1145/3091478.3091494>

1 INTRODUCTION

Trust is a vital social construct that has drawn attention from multiple areas of research including sociology, psychology, management, economics, political science and computer science. The economist Arrow [33] identifies trust as “a lubricant of the social system”, while computer scientists such as Massa et al [41] define it as a user’s opinion on another user’s characteristics. With the rise of Web 2.0 technologies, trust has emerged as a key concept in social network and social media analysis, reflecting credibility and reliability for the multitude of online participants and data [17].

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

WebSci '17, June 25-28, 2017, Troy, NY, USA

© 2017 Copyright held by the owner/author(s). Publication rights licensed to Association for Computing Machinery.

ACM ISBN 978-1-4503-4896-6/17/06...\$15.00

<https://doi.org/http://dx.doi.org/10.1145/3091478.3091494>

In particular, wireless technologies and social networking tools (e.g. Facebook) have created *citizen sensing*, appearing in CNN iReports and Twitter event commentary. Clearly, the organizational effectiveness of such resources depends on the filtering, integration and dissemination of *trustworthy* information [47]. Emergency response provides an ideal domain for examining citizen sensing [11]. Citizen response can have an enormous influence on the societal impact (cost, recovery) of a disaster. Victims and their neighbors share timely information (e.g. flood level, road blockages) and offer resources (e.g. vehicles, food and supplies) on social media, leading to the prioritization of relief effort ranging from critical infrastructure repair to saving lives in affected areas. Affordability, reach, proximity and timeliness make social media such as Twitter an attractive resource for capturing public observations and activity during emergencies [40]. However, message recipients such as response agencies must trust citizen sources to provide reliable information, and must rapidly vet and separate noise (inaccurate information from unreliable sources or ambiguities from reliable sources) from the informative signal. A trust ranking of participants in social networks can promote reliance on trustworthy citizens to improve disaster response and recovery efforts [56].

Our primary focus here is on trust among users as opposed to trust in *facts*, e.g. road closures. We adopt the notion of interpersonal trust proposed by Kelton et al [31] who consider dyadic trust as a social tie between two individuals. We only consider information that is available or can be inferred from the social network and do not take into account any detail regarding background or previous history of entities. We develop an unsupervised algorithm to predict user trust relationships in social networks, using both structural properties of the network and information content posted by members of these networks.

A key contribution of our work is a robust method that takes into account indicators of influence as a proxy for how much one user trusts another: structural cohesion within a network, and valence-enhanced content (sentiment expressed related to the concept being sensed). Taking valence into account provides a robust and stable model of trust in such an analysis. To the best of our knowledge, *this is the first unsupervised effort taking into account social theories related to influence, passive cohesiveness (structural cohesion) and active cohesiveness (valence and content) and their role on interpersonal trust*. We show that our method detects pairwise and global user trust relations on a range of real-world crisis and non-crisis datasets and outperform extant state-of-the-art methods. We also find it effective in *dynamically* identifying trustworthy users in situations of crisis or emergency.

WebSci '17, June 25-28, 2017, Troy, NY, USA

2 METHODOLOGY

Informally, we seek to develop a model to infer trust among users within a network and also identify highly trusted users or organizations within a social network. Specifically, we focus on the social network *Twitter*.

2.1 Problem Statement

Formally, we assume the social network of interest is represented as a bipartite graph $G = (U \cup T, E)$, where U and T are two disjoint sets and E is the set of edges or interactions between them. U represents the set of individuals or users in the network and T refers to the set of general topics expressed by the users in their textual content. Topics are extracted after aggregating the text posted by the users, by employing standard topic modeling algorithms based on Latent Dirichlet Allocation [9] or Non-Negative Matrix Factorization [59]. The trust prediction algorithm aims to predict the pairwise trust value between every pair of users, and generate an aggregated rank ordering of network users based on this trustworthiness score.

Our solution desiderata include the goals of efficacy and efficiency: Efficacy in effectively identifying and ranking trustworthy users and efficiency in being able to compute these in real-time emergent situations (e.g. during or shortly after a disaster). We discuss below three elements informed by social and psychological theory, that we believe play a role in developing trust between two users in a social network, and we measure these elements to determine a trust metric among users.

2.2 Influence

Theory: Leading sociologists note that trust is integral to social influence [16, 37, 50]. A messenger more easily influences or persuades a recipient to respond in a certain manner if that recipient trusts the original messenger. While trust itself is difficult to measure outside of specific experimental paradigms (for instance Berg's trust game [8], which addresses this problem from the perspective of behavioral economics), several researchers have tackled the problem of detecting *influential* users within a social network.

Here we exploit influence as a proxy for pairwise trust relationships. Theory suggests a strong correlation between the trust of a user x on a user y and the observed influence of user y on user x . Intuitively, users trust the users who influence them to re-post (or retweet) a particular post or tweet on a certain topic. The available measures of influence include the use of the structure of the network such as page-rank style [44], the dynamics of the network interaction [15], the frequency with which the users' posts are re-posted while accounting for user passivity and prior content history of the users' posts [48] or by taking into account the local neighborhood of the posting user via viewpoint analysis [4].

Implementation: Guided by the above theory and the available measures of social influence, we settled on the Influence-Passivity algorithm [48]. It is simple and also accounts for user passivity i.e. the likelihood of a user reacting to a messenger. Passivity is an essential constituent of the influence computation because intuitively, the retweeting or re-posting of a user's tweet should carry more weight from a typically passive user (who rarely retweets) than

from a relatively active or frequent retweeter. The resulting HITS-style algorithm [34] calculates a global influence and passivity score for each user.

We first construct a weighted, directed, unipartite graph $H = (U, E_h, W_h)$ consisting of all the users in set U of our bipartite graph described above, joined by a set of edges E_h and a set of edge weights W_h . Edge (i, j) exists between a user i and user j in the graph if user j re-posts or shares in some way (or retweets) a post (or tweet) posted by user i at least once. Weight w_{ij} on edge $e = (i, j)$ represents the ratio of influence that i exerts on j to the total influence i attempted to exert on j . It is expressed as $w_e = \frac{S_{ij}}{Q_i}$ where Q_i is the number of posts that user i creates and S_{ij} is the number of posts i created and j re-posted or retweeted.

The influence function $Infl_i : U \rightarrow [0, 1]$ that represents node i 's influence on the network is calculated as:

$$\begin{aligned} Infl_i &= \sum_{j:(i,j) \in E} u_{ij} Passiv_j \\ Passiv_i &= \sum_{j:(j,i) \in E} v_{ji} Infl_j \\ u_{ij} &= \frac{w_{ij}}{\sum_{(k,j) \in E} w_{kj}} \text{ and } v_{ji} = \frac{1-w_{ji}}{\sum_{(j,k) \in E} (1-w_{jk})} \end{aligned}$$

Here u_{ij} represents the amount of influence user j accepted from user i normalized by the total influence j accepted from all users in the network. v_{ji} represents the influence that user i rejected from j normalized by the total influence rejected from j by all users in the network.

2.3 Social Cohesion

Theory: Social cohesion theory posits that a necessary and sufficient condition for individuals to work as a group is cohesive social relationships among individuals within the group. While social relationships exist for different reasons (e.g. kinship ties or similar social values), we focus on a group's structural cohesion, the collective result of those various social relationships. Sociologists and public policy experts believe that if common values, *trust* or a shared sense of place emerge, they will do so as a function of structural (cohesive) engagement [37]. Similar ideas are also posited by Golbeck and Ziegler et al [20, 60]. We adopt the definition by Lott and Lott [39] that interprets cohesiveness as a function of interpersonal attraction between individuals. In other words, cohesiveness relates to the members of a group who share emotional and behavioral characteristics with one another and the group as a whole [39, 46].

Implementation: We compute the Jaccard similarity metric [13, 19] between the neighborhoods of pairs of users in the bipartite network. This approximates the number of triads each pair belongs to, or the local triangle density. The notion of triads has been widely used to characterize community cohesiveness within a network [23, 24]. Such measures are also easy to approximate efficiently [49]. Based on the above theoretical insights, two users can be said to belong to a 'group' or possess some similar behavioral characteristics if they share common contextual interests. Specifically, we associate with each user x a *vector* V_x of topic identifiers to which x has a directed edge i.e. all topics on which a user shares

text online. The Jaccard similarity between the users x and y is then:

$$Jacc(x, y) = \frac{|V_x \cap V_y|}{|V_x \cup V_y|}$$

In measuring shared topic interests among users we rely on what the social science literature refers to as passive cohesive interactions [37, 39]. We next examine the role of active relationships, which account for specific content, popularity of said content and the emotional attachment (sentiment/valence) associated with such content by actors within such networks.

2.4 Valence

Theory: We hypothesize that a critical dimension in the trust equation is the positive interactions, i.e. supportive exchanges among individuals and more broadly among communities, or “active social relationships”. Such contacts and connections reflect trust as they offer people and organizations mutual support, information and credit. This is particularly relevant during times of need; such as those that arise in crisis and disaster settings [37]. The Jaccard measure just described largely reflects similarity between users in the social network based on structural cohesion. It does not account for the popularity of certain topics that the users talk about, nor as suggested by Lott and Lott [39] does it account for emotional content (valence ranging from positive to negative) and interpersonal agreement among users. We note that to the best of our knowledge, while the corresponding social theory exists, none of these have been examined in the context of online social networks. To overcome the limitations of the Jaccard measure, we propose a more nuanced measure that takes into account the relative *popularity* of the topics that the tweets or text of the users primarily describe, the valence of a user with respect to a particular topic and the agreement among them.

Implementation: We introduce the notion of a *shared* topic (or context) between two users in U as any topic in T to which both users in graph G have a directed edge. Our implementation accounts for a number of confounding influences on apparent sharing. We distinguish between shared topics according to their relative popularity, i.e. their in-degree in the bipartite graph. Intuitively, as the in-degree of a topic (the number of users talking about it) increases, the extent to which we can infer about the relative similarity of two users who post on that topic reduces. Two users who post on a rare topic are more likely to have an affinity or an interest towards that topic and consequently towards each other and therefore, a stronger trust relationship. Nevertheless, a pair of users posting on a popular topic may be doing so precisely because of its popularity or it being the current trend (see Figure 1(a)). User baseline activity level is also relevant. If two users post frequently on numerous or diverse topics, sharing a topic may not attest as much to their similarity (see Figure 1(b)) as for a pair of less active users sharing a common topic. Figure 1(c) thus represents the case in which the pair of users x and y have the strongest likelihood of being similar to each other (and consequently trusting each other) based on their textual content. We now formalize the notion of *degree discounting* to capture the above ideas as follows:

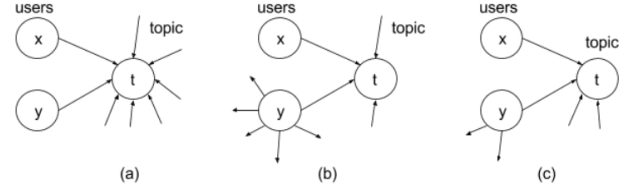


Figure 1: Content based user similarity, based on degree discounting

- (1) When two users x and y share a topic t , the contribution of t to the similarity between x and y is inversely related to the in-degree of t .
- (2) The out-link similarity between two users x and y is inversely related to the out-degrees of x and y .

$$sim_d(x, y) = \frac{1}{\sqrt{D_o(x, x)}\sqrt{D_o(y, y)}} \sum_t \frac{A(x, t)A(y, t)}{\sqrt{D_i(t, t)}}$$

$sim_d(x, y)$ is the degree-discounted out-link similarity between users x and y . A is the adjacency matrix of the bipartite graph G . D_o is the diagonal matrix of users' out-degrees and D_i is the diagonal matrix of topics' in-degrees in G . t represents a shared topic between x and y , and can be defined in two ways: i) *without valence*: the pair of users merely post text or tweets on t , and ii) *with valence*: they not only post on t but also express the same dominant valence towards it (positive, negative or neutral) in their text.

The inclusion of valence expressed by the users on a particular topic lends more validity to pairwise user similarity and may reflect greater trust between a pair of users, reflecting the theoretical notion of interpersonal emotional agreement. A user x likely has greater trust in a user y who shares x 's opinion on a particular event or topic. To quantify the overall opinion or valence within the textual content expressed by each user on each topic, we use a widely used tool called SentiStrength [55]. It builds a simple discriminative predictor based on psychological theories of emotive strength, exploiting de-facto grammar and spelling styles (e.g. informal spellings, social media specific linguistic terms, idioms and emoticons). We found this tool to be more effective than traditional ones such as LIWC [45] and ANEW [10] that are better suited to longer and more linguistically standard pieces of text.

2.5 Putting It All Together

To combine the three measures or quantities (influence, cohesion and valence), we first did a systematic study across a range of datasets described in Tables 1 and 2. We observed that each of these measures are well estimated by a Gaussian distribution suggesting that a natural way to standardize these quantities is to employ z-score normalization [35].

Once each measure is normalized we determine the regularization coefficients (via a parametric grid search as described in the next section) employed in the overall trust equation as follows:

$$Trust(x, y) = \alpha Infl(y, x) + \beta Jacc(x, y) + \gamma sim_d(x, y)$$

$Trust(x, y)$ represents the pairwise trust of user x on user y . α , β and γ are regularization parameters representing the factor weights and are tuned empirically such that $\alpha + \beta + \gamma = 1$.

WebSci '17, June 25-28, 2017, Troy, NY, USA

After computing the value of pairwise trust for every pair of users, we assign a global trust score $GTrust(x)$ to each user x in the following way:

$$GTrust(x) = \frac{\sum_{y \in T_x} Trust(y, x)}{|T_x|}$$

T_x = a set of users that have a non-zero pairwise trust score with user x , $|T_x|$ = cardinality of set T_x .

Based on these global trust scores assigned to users, we generate a trust-based ranking of all the users in the dataset. The relative order of $GTrust$ values provides a notion of ordinality regarding the overall trust a user enjoys within these network contexts. Depending on the values of α , β and γ employed to compute pairwise trust, we obtain multiple distinct trust-based user rankings.

Complexity Considerations: In order to compute a trust score between all pairs of users in the social network, a $O(n^2)$ complexity is unavoidable. Particularly for larger datasets with millions or billions of users, computing trust between every pair of users in the network will not scale, so pairwise trust might need to be only computed for a sample of users. For discovering the top trustworthy users one can potentially employ a smart sampling strategy where the trust for each user is accumulated over a sample of other users that interact with that user. Strategies such as those employed in similarity search problems [13, 19] can also be leveraged.

In our algorithm, the complexity of computing individual factors is as follows: Computing influence has the same complexity as the HITS algorithm [34] i.e. $O(E)$ per iteration; in our experiments we typically converge in less than 30 iterations. The complexity of determining the structural cohesion of two users as well as the valence step is bounded again by $O(E)$ (although in practice it is much less with our proposed optimizations). The complexity of parametric tuning (for each of the factors of influence, cohesion, and valence) can potentially be expensive. However, as discussed next, our results strongly suggest a robust weighting scheme highlighting the importance of influence, followed by content valence, followed by passive social cohesion.

3 EVALUATION

3.1 Datasets and Ground Truth

The datasets we employ in this study are described in Tables 1, 2 and 3. All social media data were collected using Twitter’s Streaming API. Because ground truth for each pairwise trust relationship from social media data is difficult to obtain without a dedicated social survey instrument, we also include results on two datasets with normative ground truth: i) a Film DVD review dataset collected by Guo et al [26] in December 2013 by crawling 17 categories of film DVDs from the dvd.ciao.co.uk website; and ii) a dataset made available by Massa et al from the Epinions product rating and review website [42]. Both these datasets provide authentic ground truth information as a list of pairs of users who trust each other (scaled values from 1 to 5). We construct a bipartite graph for these two datasets as described in Section 2. Because there is no direct measure of re-posting or retweeting associated with these two datasets, for the purpose of computing influence we assume that a user x functionally ‘retweets’ a user y if x rates y ’s reviews more than three times. For contextual information, we used the provided genre of each film and the provided category of each product

Nikhita Vedula, Srinivasan Parthasarathy, and Valerie L. Shalin

Dataset	#Users	#Topics	#Nodes	#Edges	#Tweets
India Anti-Corruption	2104	15	2119	7180	100K
Mumbai Blast	581	10	591	932	10K
Phone and Tablet	9939	15	9954	16265	100K
Houston Floods	986	15	971	875	100K
Hurricane Irene	50561	20	50541	17593	200K
Nice Attack	253243	20	253223	166943	800K

Table 1: Bipartite graph statistics of social media datasets

Dataset	#Users	#Topics	#Nodes	#Edges	#Trust relations
CiaoDVD	7375	17	7392	111781	40133
Epinions	114467	27	114494	442787	717667

Table 2: Bipartite graph statistics of non-social media datasets with ground truth trust relations

Dataset	Timeline
India Anti-Corruption	April 4, 2011 to December 28, 2011: Protests against political corruption in India (https://en.wikipedia.org/wiki/2011_Indian_anti-corruption_movement)
Mumbai Blast	July 13, 2011: A series of three coordinated bombings in Mumbai (https://en.wikipedia.org/wiki/2011_Mumbai_bombings)
Hurricane Irene	August 21, 2011 to August 30, 2011: A tropical cyclone on US East Coast that grew into a hurricane (https://en.wikipedia.org/wiki/Hurricane_Irene)
Phone and Tablet	All tweets related to phones and tablets, during the day of April 15, 2013
Houston Floods	April 15, 2016 to April 23, 2016: Snowstorm leading to severe floods (https://en.wikipedia.org/wiki/2016_Texas_floods)
Nice Attacks	July 14, 2016: A cargo truck driven into a crowd, followed by a gunfire which led to an emergency (https://en.wikipedia.org/wiki/2016_Nice_attack)

Table 3: Timeline and details of each Twitter dataset

respectively, as topics. Additionally, we used user provided ratings to estimate the user valence towards a particular film or product. A user rating of 4 or more (out of 5) was taken as the expression of positive valence, 2 or less was taken as negative valence and a rating of 3 was assumed to be neutral.

3.2 Factor Analysis and Impact of Valence

Metrics: We begin by comparing our global trust-based user ranking (details in Section 2.5) at various parameter value settings against the ground truth user trust ranking for the CiaoDVD and Epinions datasets. This provides an independent assessment of our method on datasets with factual ground truth. For this, we made use of the standard information retrieval metric of Normalized Discounted Cumulative Gain (NDCG) [28]. NDCG is often the measure

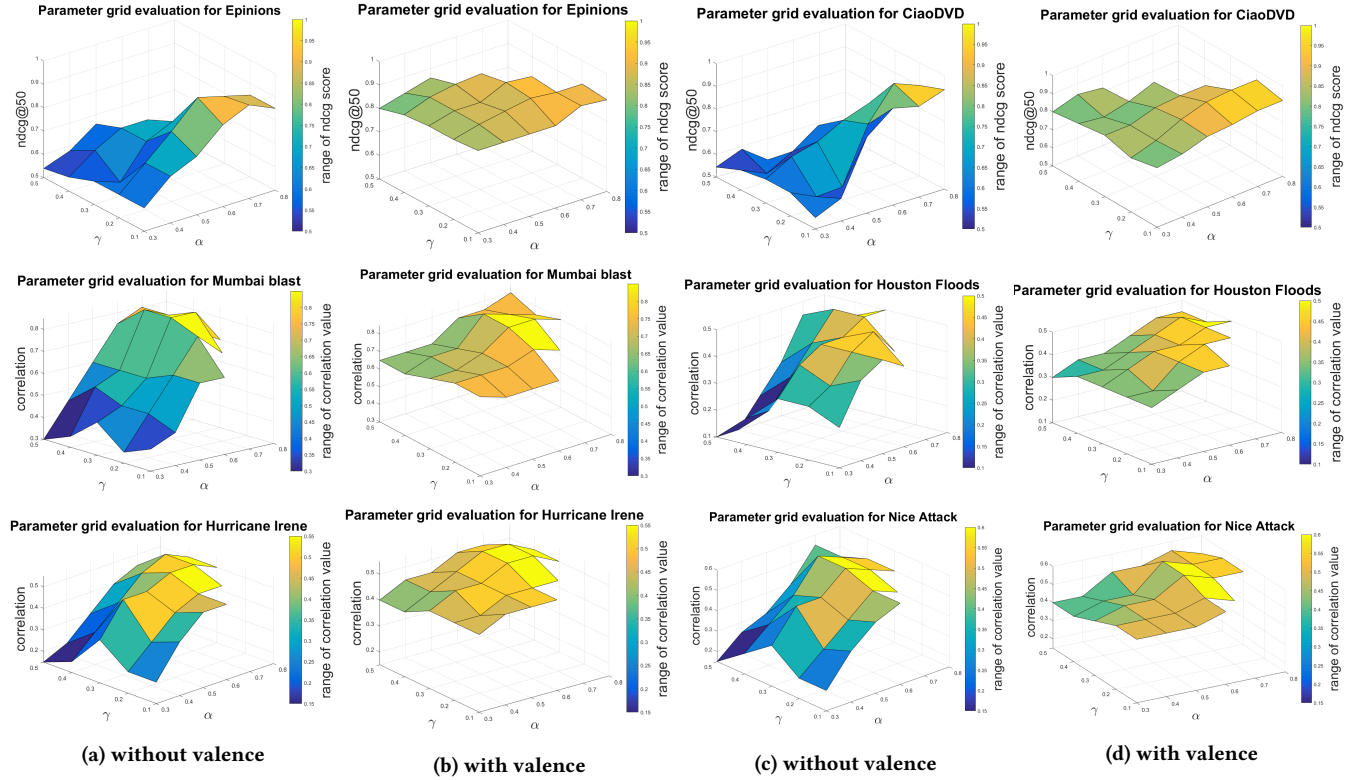


Figure 2: The first row of sub-figures shows the NDCG scores of various rank orders for the parameter grid against ground truth for CiaoDVD and Epinions. The next 2 rows show correlation between the pairwise trust score and conversation length for the parametric grid for social media datasets; in both cases using content-based similarity without and with valence

Dataset	α	β	γ
India Anti-Corruption	0.6	0.05	0.35
Mumbai Blast	0.65	0.05	0.3
Phone and Tablet	0.7	0.2	0.1
Houston Floods	0.65	0.1	0.25
Hurricane Irene	0.65	0.05	0.3
Nice Attacks	0.7	0.05	0.25
CiaoDVD	0.7	0.1	0.2
Epinions	0.65	0.1	0.25

Table 4: Best parametric settings for different datasets

of choice for comparing ranked lists since it emphasizes high fidelity with ground truth ranking at the top of the list [28], which aligns with our goals for identifying top trusted users in emergent situations. The NDCG score at a rank position k (we used $k = 50$ in our experiments) is defined as:

$$DCG_k = \sum_{i=1}^k \frac{2^{imp_i} - 1}{\log_2(i+1)}$$

$$NDCG_k = \frac{DCG_k}{ideal_k}$$

where imp_i is an integer (between -2 and 2 based on the position of the user in the original rank list) representing the importance of user i , DCG_k is the discounted cumulative gain at rank k and $ideal_k$ is the ideal ground truth ranking.

For social media data, ground truth information on pairwise trust is difficult to obtain, which requires us to identify an approximation to ground truth. Adali et al [1, 2], recommend the use of the length of conversation between pairs of users as an approximate measure of the mutual trust between them. We acknowledge that there can be two limitations of such an approximation. First, the absence of dialogue online between a pair of users does not imply a lack of trust (false negatives). Roughly 35% of the users on average do not engage in active conversation during the respective time period of the events. Second, conversation length could also reflect discord as opposed to agreement or trust (false positives). We manually scrutinized the crisis related Twitter data in detail and found no evidence of lengthy discordant conversations; contextually, in such situations, discord is unlikely to occur. The conversation lengths in the datasets range from 2 to 13.6 on average. We computed the Pearson correlation coefficient between the length of a conversation between a pair of users (i.e. the number of times they replied to each others tweets during the time period of the particular event), and the corresponding trust score obtained by our methodology. As Table 7 and the last two rows of Figure 2 show, moderate (0.45) to strong (0.85) correlations were obtained between trust scores and conversation length, which indicates that this metric can be a suitable approximation despite the limitations noted above. We also note that conversation length was not used for computing any

WebSci '17, June 25-28, 2017, Troy, NY, USA

of the factors in our trust equation, it is an independent measure of quality.

Results: Figure 2 illustrates a series of surface heat plots varying two parameters: α and γ (β can be inferred from them). The first row of plots shows the variation in NDCG scores while the next two rows of plots show the variation in the correlation between pairwise trust score and conversation length, as the parametric values are varied, with and without valence. We find that the *inclusion of valence reduces the sensitivity of the method to parametric tuning in both cases*. Without valence, the NDCG scores range from 0.55-1 with high fluctuations on small parametric changes, whereas with valence the decision surface is more stable (the NDCG scores range from 0.75-1). We found the best NDCG score of 0.955 for CiaoDVD and 0.913 for Epinions (see Table 4 for parameter values). The surface plots for the social media datasets show similar trends: i) moderate (0.45) to strong (0.85) correlation between obtained trust values and conversation length demonstrating the effectiveness of our method; and ii) valence plays a critical role in a performance improvement and stabilizing the sensitivity of the method to parametric changes i.e. reducing fluctuation in correlation scores for small parametric changes. For the social media datasets, the best correlation values obtained by our method can be viewed in Table 7.

For each dataset, the best parametric setting is noted in Table 4, used henceforth for all experiments unless otherwise stated. Scanning through this table, it is clear that influence is the strongest factor contributing to an accurate ranking; α values typically range between 0.6 and 0.7. Content-based user similarity conditioned on topic popularity and valence weighted by γ follows, with parameter values typically between 0.2 and 0.3. Finally, structural cohesion had a non-trivial but muted role with β values up to 0.2.

3.3 Comparative Analysis

Baselines: We evaluated our method's performance on the CiaoDVD and Epinions datasets against the following unsupervised baseline trust computation algorithms: EigenTrust by Kamwar et al [29], TidalTrust by Katz et al [30] and an atomic trust propagation based approach by Guha et al [25]. We additionally include as baselines algorithms that only compute social influence to evaluate how they fare against trust computation; namely, a topic-aware influence maximization approach [3] called INFLEX, and a modification of our method to consider only the influence component i.e. setting the value of the parameter α to 1. Although our method is unsupervised, for the sake of completeness we further compare our method with a recently proposed supervised algorithm ETD [7], which also uses emotional information to aid in trust prediction, and is shown to outperform other supervised trust prediction methods [27, 38]. While such algorithms are hard to deploy in a social media setting (as obtaining ground truth for trust relationships is difficult), and moreover expensive to compute, they provide a challenging baseline.

Results: In Figure 3, the x axis represents the rank at which we compute the NDCG score between the global ranking developed by the trust algorithm and the ground truth trust ranking, and the y axis represents the value of the NDCG score. Since we lacked the timestamp at which users posted and rated reviews for the CiaoDVD dataset, which is required for influence maximization

Nikhita Vedula, Srinivasan Parthasarathy, and Valerie L. Shalin

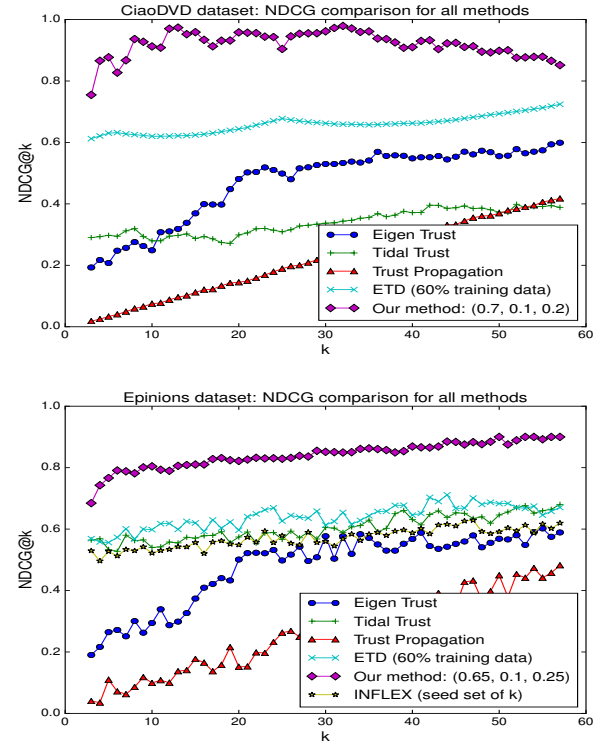


Figure 3: Comparison of NDCG score at various ranks for our algorithm against baselines, for CiaoDVD and Epinions.

algorithms, we could not run the INFLEX algorithm on this dataset. We observe that our method outperforms the baseline techniques, including the supervised method, giving a consistently high NDCG score > 0.75 .

In order to assess the quality of pairwise user trust relations our algorithm is able to detect, we next compute the F-measure or F-score for the baseline algorithms and our method as follows:

$$P = \frac{TP}{TP+FP}$$

$$R = \frac{TP}{TP+FN}$$

$$Fscore = \frac{2PR}{P+R}$$

Here, TP stands for the number of pairwise user trust relations correctly recognized by the algorithm (true positives), FP represents the number of relations identified as trusted by the algorithm, but which are either distrust relations or those for which ground truth is not available (false positives) and FN stands for the number of pairwise trust relations the algorithm failed to recognize (false negatives). P and R represent the precision and recall respectively. We consider a reasonable trust relation to exist between two users if the value of the (normalized) pairwise trust between them is ≥ 0.5 .

We find from Tables 5 and 6 that our unsupervised framework outperforms all baseline algorithms significantly with respect to NDCG scores at rank 50, for both the social media and non-social media datasets. Adding content and valence information while computing trust does improve NDCG scores, showing that it is insufficient to

consider only influence propagation while computing trust. Since EigenTrust, INFLEX and the influence component of our method (α set to 1) only compute a global and not pairwise trust score for each user, we are unable to compute an F-score for them. *With respect to the available F-scores, our method outperforms all unsupervised baselines and is comparable to the supervised ETD approach*, when it trains on 60% of pairwise trust values (it outperforms the ETD approach with 30% training data). Clearly, it is impractical to obtain such a large fraction of ground truth pairwise trust data from even a moderately sized social network.

Algorithm	Dataset	NDCG@50	F-score
EigenTrust	CiaoDVD	0.523	N/A
TidalTrust	CiaoDVD	0.35	0.43
TrustPropagation	CiaoDVD	0.33	0.21
ETD-T60 (T30)	CiaoDVD	0.69 (0.489)	0.78 (0.53)
Our method ($\alpha = 1$)	CiaoDVD	0.686	N/A
Our method	CiaoDVD	0.955	0.84
EigenTrust	Epinions	0.494	N/A
TidalTrust	Epinions	0.586	0.465
TrustPropagation	Epinions	0.371	0.237
ETD-T60 (T30)	Epinions	0.645 (0.51)	0.816 (0.52)
INFLEX	Epinions	0.579	N/A
Our method ($\alpha = 1$)	Epinions	0.658	N/A
Our method	Epinions	0.913	0.805

Table 5: NDCG at rank 50 and F-score values for different algorithms for CiaoDVD and Epinions. ETD results are reported with 30% (T30) and 60% training (T60) data.

Algorithm	Avg NDCG@50 for Twitter datasets	Avg F-score for Twitter datasets
EigenTrust	0.444	N/A
TidalTrust	0.549	0.511
TrustPropagation	0.321	0.303
INFLEX	0.647	N/A
Our method	0.876	0.803

Table 6: NDCG scores at rank 50 and F-scores averaged across the Twitter datasets, for the unsupervised algorithms using conversation length as ground truth.

Dataset	Corr (Tidal Trust)	Corr (Trust Propagation)	Corr (Our Method)
India Anti-Corruption	0.35	0.16	0.507
Mumbai Blast	0.521	0.187	0.849
Phone/Tablet	0.309	0.083	0.4614
Houston Flood	0.267	0.111	0.484
Hurricane Irene	0.222	0.091	0.518
Nice Attacks	0.313	0.181	0.565

Table 7: Correlation between pairwise trust score and conversation length between pairs of users during that time period, using different algorithms

For social media datasets, in Table 7 we report the correlation between conversation length and pairwise trust scores computed by our method and the unsupervised baselines (supervised baselines are not feasible because we lack pairwise trust ground truth). As before, we observe that our method outperforms the baselines significantly.

3.4 Performance Enhancements and Scalability

Benefits of Degree-Discounting: Here we examine the benefits of accounting for degree-discounting while computing pairwise user trust (Figure 1). The user trust relations obtained without this optimization achieve an NDCG@50 score of 0.76 and an F1-score of 0.424 on the CiaoDVD dataset. Adding degree discounting without valence yields an NDCG@50 score of 0.82 and F1-score of 0.63 respectively. Further, adding valence yields an NDCG@50 score of 0.955 and an F1-score of 0.84 respectively. Similar benefits were observed in other datasets.

Execution Time: We present an analysis of the total runtime of our method amortized over the number of user pairs in Table 8. We note that using SentiStrength for detecting valence (which can process about 10K tweets per second), the efficiency of computing pairwise trust is comfortably able to handle the influx of tweets associated with an event even at full firehose (several hundred million tweets a day) rates.

Dataset	Runtime per pair of users
India Anti-Corruption	0.000854 sec
Mumbai Blast	0.0034 sec
Phone and Tablet	6.56×10^{-4} sec
Houston Floods	0.000296 sec
Hurricane Irene	6.689×10^{-5} sec
Nice Attacks	4.659×10^{-6} sec
CiaoDVD Film	0.000199 sec
Epinions	9.616×10^{-6} sec

Table 8: Runtime for pairwise trust value computation and parameter tuning, amortized over number of user pairs

3.5 Case Study: Crisis Response

Here, we examine the kinds of individual users or organizations on Twitter who were identified by our algorithm as being highly trustworthy during various hazards, and also track the change in their overall trustworthiness across different temporal phases of the hazard occurrence, i.e. before the hazard, during its worst impact and immediately after it has subsided at the affected area. Due to space constraints, we only display results for three hazard datasets in Table 9. Users common across columns are represented in the same color (except black) so that we can track how their trust ranking changes across the three phases of the hazard. Top trustworthy users unique to each phase are colored in black.

Observations: Several users in Table 9 are well known personalities or reputed organizations and are thus likely to be highly

WebSci '17, June 25-28, 2017, Troy, NY, USA

Nikhita Vedula, Srinivasan Parthasarathy, and Valerie L. Shalin

Before	During	After
mashable	cnnbrk	cnnbrk
lfmcullough	BreakingNews	BreakingNews
richmintz	USArmy	BarackObama
Reuters	CharityIdeas	nytimes
FrommersTravel	severestudios	HumaneSociety
nydailynews	shibanijoshi	RedCross
6abc	JimCantore	JimCantore
travelingmoms	xanpearson	atmanes
severestudios	CraigatFEMA	CraigatFEMA
BreakingNews	MikeBloomberg	Fanua
Daily_Press	atmanes	RedCrossPhilly
cnnbrk	Fanua	SamaritansPurse
funnyordie	HumaneSociety	RedCrossSAZ
afreedma	BarackObama	mashable
BarackObama	RedCross	USGS

(a) Hurricane Irene

Before	During	After
GlitchxCity	Breaking911	Breaking911
Sportsnaut	NWSHouston	NWSHouston
TriCityHerald	AlertHouston	BarackObama
Nick_Anderson_	WSOCWeather	AlertHouston
HOUBizJournal	StormViewLIVE	<i>TexasTsunami</i>
StarfishGawdness	BarackObama	RedCross
Breaking911	ArchCollegeTAMU	ArchCollegeTAMU
BarackObama	JohnCornyn	WSOCWeather
JohnCornyn	<i>TexasTsunami</i>	JohnCornyn
NWSHouston	GlitchxCity	GlitchxCity

(b) Houston Floods

Before	During	After
ScepticGeek	ndtv	mid_day
AltCricket	mid_day	ndtv
acarvin	rameshshrivats	htTweets
dina	maheshmurthy	rameshshrivats
maheshmurthy	AnupamPKher	<i>ashwinsid</i>
htTweets	htTweets	Netra
mid_day	fakingnews	fakingnews
ndtv	PatrickMeier	maheshmurthy
timesofindia	<i>ashwinsid</i>	PatrickMeier
guardian	Netra	ScepticGeek

(c) Mumbai Blast

Table 9: Top trustworthy users with global trust score > 0.7 for different datasets. The same color is used for users reappearing across the phases of a disaster. Newly emergent trustworthy users are italicised.

trusted. These include journalists and news agencies (*cnnbrk*, *BreakingNews*, *Breaking911*, *ndtv*), key weather related officials and services (*NWSHouston*, *CraigAtFEMA*, *JimCantore*), entertainment related (*mashable*, *funnyordie*, *GlitchxCity*), political and social figures (*BarackObama*, *xanpearson*, *dina*) and relief organizations (*SamaritansPurse*, *RedCross*, *HumaneSociety*). This lends credibility to our analysis.

Moreover, certain users were not previously well known in any field, yet our algorithm identified them as commanding a high trust value during the time period of these events. Such users have been highlighted in *italics* in Table 9. On examining their tweet logs, we found that the Twitter user *TexasTsunami* provided assistance to the Houston flood victims and tweeted some strong statements such as “*I know it is ILLEGAL to give a hungry man a sandwich here in Houston. Is it legal to assist flood victims?*”, which popularized him and increased his trust level on topics related to the flood (though he wasn’t as popular as the other highly trusted users). Similarly, user *atmanes* helped a taxi service in transporting animals, while user *Fanua* repeatedly re-tweeted several reliable news sources regarding Hurricane Irene, which increased the trust of other users towards them during this time. User *ashwinsid* provided transport to stranded victims of the Mumbai blast. Thus, *our approach not only captures trusted users who are well known or popular but also effectively identifies emergent trustworthy users* who were neither well known nor previously popular – during and immediately after an emergency situation. This is particularly relevant for our ongoing efforts in identifying trustworthy “good samaritan” citizen sensors both during and immediately after a disaster occurs.

Role of Valence: Valence is crucial in recognizing emergent trustworthy users. Without valence, we observed that good samaritan, trustworthy users (*atmanes*, *Fanua*, *TexasTsunami*, *ashwinsid*) could only be detected in one of the datasets (Mumbai Blast), and that too only in the top 60 trustworthy users (and not in the top 10 or 15).

Dynamics of Trust: Finally, we perceive intuitive trends in connection with the changes in highly trusted users over the three phases of the disaster previously outlined. From Table 9 we note that before the hurricane or flood struck the respective affected area, the highly trusted users were from a wide variety of fields such as travel, sports or entertainment blogs along with key political figures and news channels. However, we see a significant variation during and immediately after the disaster. News channels, reporters and weather related user accounts rise to the top of the list. New trustworthy users start emerging in the ‘during’ phase and their trust scores rise as the disaster progresses to the ‘immediately after’ phase, which is when they primarily provide voluntary assistance to affected victims. Additionally, relief and humanitarian organizations such as the *RedCross* are highly trustworthy shortly after the disaster.

4 RELATED WORK

Existing literature addresses the challenge of identifying or predicting the credible aspects of data and entities, under a social model of trust [54]. A simple strategy to encode a pre-defined notion of trust involves learning the encoding (via regression or classification) from a labeled set of specific interactions and their associated values obtained from a domain expert. Subsequently the learned model automatically categorizes the trust values associated with other relationships within the network. Both the biological and social network analysis literatures rely on the local topology within the network to assess the confidence associated with a specific relationship [18]. However, topological signals alone may be insufficient. For example, Palen et al [56] imply that content and context, and

metrics such as re-tweeting by others reflect a notion of trust between the user and her immediate followers. Some of these signals can be directly recovered from the data (e.g. location-specific tags from Twitter, volunteered GIS information etc.) but others must be inferred through suitable content analysis and other methods [43].

We have hypothesized that the idea of expertise or influence can serve as a prominent contributor to trust. Influence can often be estimated from the structure of the global network, as in Twitter-Rank [57] and Trust-Rank [58], or the local network via viewpoint-based methods [4]. A large body of work has focused on studying diffusion and influence specifically on Twitter, using measures of influence such as number of followers, page-rank, number of retweets and number of mentions [12, 36, 57]. The influence-passivity algorithm by Romero et al [48] which we employ in this work also makes use of Twitter retweets and URLs, however it also simultaneously accounts for the passivity of network users as well, which can be important as explained in Section 2.

Social influence coupled with contextual information has been used in the literature in the problem of influence maximization [3, 6, 14, 32], where the objective is to identify seed users such that the number of users they influence in the network is maximized. We note that though influence plays a crucial role in our algorithm in quantifying trust, our work is distinct from these efforts in that we do not aim to study influence (and consequently, trust) propagation through the network or find the set of users with the maximum overall trust reach. We study both pairwise trust relations among users as well as identify users who are globally trusted. Having said that, we do compare our work against the topic-aware influence maximization algorithm by Aslay et al [3] and find that along with influence and context, shared content and valence information play a non-trivial role in discerning trust among users (Sections 3 and 3.5).

One may not have enough data or domain knowledge to assess a meaningful trust value for all of the entities and relationships in the network. Hence, propagating trust values across entities using a set of rules [25] may be essential to obtain a completely specified trust network. Golbeck and Hendler [22] describe some of the challenges with trust propagation (including conflict resolution) based on the underlying model of trust and highlight the following properties regarding trust propagation: asymmetry (person A may trust person B but not vice-versa), transitivity (if person A trusts person B and person B trusts person C, a trust relationship can be inferred between A and C) and composability (a user should aggregate trust values received from different paths). The TidalTrust algorithm [21] propagates trust ratings along a path between a source and a sink in Friend-Of-A-Friend based social networks using a Breadth-First search. EigenTrust [29] and MoleTrust [41] are peer-to-peer algorithms for determining peer trustworthiness.

A crucial dimension to the study of trust is the fact that trust is context-dependent; different users may be trusted differently on different contexts or topics. Tang et al [53] in their work on mTrust develop a topic-specific tensor representation in which a user probabilistically trusts another on a certain topic. In our work, we incorporate contextual information as a contributor to pairwise user trust scores but we do not currently compute topic-specific user trust values. We also utilize the idea that similarity in emotion

expressed by users can be a crucial signal of the trust between them, which has also been studied in [7].

Finally, the notion of structural similarity between users has a role to play in shaping their trust relationships. Tajfel [51] defines the concept of social identity as “the individual’s knowledge that he belongs to certain social groups together with some emotional and value significance to him of this group membership”. Such shared identity among members of a group can in turn lead to cohesiveness, uniformity and the motivation to sustain the reputation of their associated identity, which can consequently increase the feeling of mutual trust and affinity among the group members. In the literature, Golbeck [20] supports the idea of a positive correlation between user profile similarity and personalized trust values, while Yeung et al [5] find similarities in user trust networks on product review sites. Tang et al [52] model the effects of homophily in trust prediction with a low rank matrix factorization model. We incorporate this concept into our trust calculation by increasing the pairwise trust score between users if they belong to a “group”, i.e. if they share a common context.

5 CONCLUDING REMARKS

We present a simple unsupervised approach to computing interpersonal trust among users within a social network, bringing to bear theoretical ideas from psychology and sociology as they relate to influence, passive (structural) and active cohesiveness (content and valence). In our empirical analysis we sought to answer three questions: i) Which among the three factors (influence, structural cohesion, affective valence) are most important to estimate trust relationships among users in a social network? ii) How robust is the method in predicting trust with and without valence? iii) How does real-world performance of the method compare to baselines and can it be useful in emergent settings?

Consistent with the literature, although we find influence to be the principal factor contributing to recognizing trustworthy users in social media, we demonstrate that the presence of valence or sentiment while calculating trust adds significantly to the stability of the response surface, and to performance. Structural cohesion, while still useful has less of an impact than the other two factors, especially in the case of ephemeral (Mumbai attacks, Nice attacks, Hurricane Irene and Houston Floods) and political movement events (India Anti-Corruption). This may be related to the type of event, because structural cohesion plays a stronger role than valence-enhanced content on the Phone and Tablet dataset. Finally, we demonstrate that our method is able to develop a trust based ranking of users that comprehensively outperforms strong baselines on a range of real-world datasets. We also demonstrate the efficacy of the methodology for the dynamic identification of trusted users in emergent crisis settings.

Future Work: We plan to further examine the temporal dynamics in user trust relations. We are enhancing our evaluation to examine broad spectrum effects of our trust inference procedure, in particular the propagation of trust when limited ground truth is available to our method (unavoidable with social media data). We also plan to model user trust relations over a hierarchy of topics and use more sophisticated techniques such as word embeddings for valence. Although our results reveal reasonably stable parametric settings for

WebSci '17, June 25-28, 2017, Troy, NY, USA

influence, cohesion and valence-enhanced content across datasets, there is some variance. We would like to develop a method to auto-tune the parameters of our method in the future. We also plan to enhance our study with a detailed survey instrument that polls individual users regarding their trust relationships. Such ground truth can provide a broader evaluation for not just the top trustworthy users but also on pairwise relationships across a larger sample of users.

6 ACKNOWLEDGMENTS

This work is supported by the National Science Foundation Grant EAR-1520870. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation. The authors also thank Jiongqian Liang, T.K. Prasad and A. Sheth for useful comments on earlier drafts of this work.

REFERENCES

- [1] Sibel Adali, Robert Escriva, Mark K Goldberg, Mykola Hayvanovych, Malik Magdon-Ismael, Boleslaw K Szymanski, William A Wallace, and Gregory Williams. 2010. Measuring behavioral trust in social networks. In *IEEE ISI*.
- [2] Sibel Adali, Fred Sisenda, and Malik Magdon-Ismael. 2012. Actions speak as loud as words: Predicting relationships from social behavior data. In *WWW*.
- [3] Cigdem Aslay, Nicola Barbieri, Francesco Bonchi, and Ricardo A Baeza-Yates. 2014. Online Topic-aware Influence Maximization Queries.. In *EDBT*. 295–306.
- [4] Sitaram Asur and Srinivasan Parthasarathy. 2009. A viewpoint-based approach for interaction graph analysis. In *SIGKDD*.
- [5] Ching-man Au Yeung and Tomoharu Iwata. 2011. Strength of social influence in trust networks in product review sites. In *WSDM*.
- [6] Nicola Barbieri, Francesco Bonchi, and Giuseppe Manco. 2013. Topic-aware social influence propagation models. *Knowledge and information systems* (2013).
- [7] Ghazaleh Beigi, Jiliang Tang, Suhang Wang, and Huan Liu. 2016. Exploiting emotional information for trust/distrust prediction. In *SIAM*.
- [8] Joyce Berg, John Dickhaut, and Kevin McCabe. 1995. Trust, reciprocity, and social history. *Games and economic behavior* (1995).
- [9] David M Blei. 2012. Probabilistic topic models. *Commun. ACM* (2012).
- [10] Margaret M Bradley and Peter J Lang. 1999. *Affective norms for English words*. Technical Report. C-1, the center for research in psycho physiology, University of Florida.
- [11] Carlos Castillo. 2016. *Big Crisis Data*. Cambridge University Press.
- [12] Meeyoung Cha, Hamed Haddadi, Fabricio Benevenuto, and P Krishna Gummadi. 2010. Measuring user influence in twitter: The million follower fallacy. *ICWSM* (2010).
- [13] Moses S Charikar. 2002. Similarity estimation techniques from rounding algorithms. In *STOC*.
- [14] Wei Chen, Tian Lin, and Cheng Yang. 2014. Efficient topic-aware influence maximization using preprocessing. *CoRR, abs/1403.0057* (2014).
- [15] Pedro Domingos and Matt Richardson. 2001. Mining the network value of customers. In *SIGKDD*.
- [16] Rino Falcone and Cristiano Castelfranchi. 2001. Social trust: A cognitive approach. In *Trust and deception in virtual societies*.
- [17] BJ Fogg and Hsiang Tseng. 1999. The elements of computer credibility. In *SIGCHI*.
- [18] Santo Fortunato. 2010. Community detection in graphs. *Physics reports* (2010).
- [19] Aristides Gionis, Piotr Indyk, Rajeev Motwani, and others. 1999. Similarity search in high dimensions via hashing. In *VLDB*.
- [20] Jennifer Golbeck. 2009. Trust and nuanced profile similarity in online social networks. *TWEB* (2009).
- [21] Jennifer Golbeck and James Hendler. 2006. Filmtrust: Movie recommendations using trust in web-based social networks. In *IEEE CCNC*.
- [22] Jennifer Golbeck and James Hendler. 2006. Inferring binary trust relationships in web-based social networks. *TOIT* (2006).
- [23] Debra S Goldberg and Frederick P Roth. 2003. Assessing experimentally derived interactions in a small world. *Proceedings of the National Academy of Sciences* (2003).
- [24] Mark S Granovetter. 1973. The strength of weak ties. *American journal of sociology* (1973).
- [25] Ramanathan Guha, Ravi Kumar, Prabhakar Raghavan, and Andrew Tomkins. 2004. Propagation of trust and distrust. In *WWW*.
- [26] G. Guo, J. Zhang, D. Thalmann, and N. Yorke-Smith. 2014. ETAF: An Extended Trust Antecedents Framework for Trust Prediction. In *ASONAM*.
- [27] Cho-Jui Hsieh, Kai-Yang Chiang, and Inderjit S Dhillon. 2012. Low rank modeling of signed networks. In *ACM SIGKDD*.
- [28] Kalervo Järvelin and Jaana Kekäläinen. 2002. Cumulated gain-based evaluation of IR techniques. *TOIS* (2002).
- [29] Sepandar D Kamvar, Mario T Schlosser, and Hector Garcia-Molina. 2003. The eigentrust algorithm for reputation management in p2p networks. In *WWW*.
- [30] Yarden Katz and Jennifer Golbeck. 2006. Social network-based trust in prioritized default logic. In *AAAI*.
- [31] Kari Kelton, Kenneth R Fleischmann, and William A Wallace. 2008. Trust in digital information. *JASIST* (2008).
- [32] David Kempe, Jon Kleinberg, and Éva Tardos. 2003. Maximizing the spread of influence through a social network. In *SIGKDD*.
- [33] Arrow Kenneth and others. 1974. The limits of organization. *N-Y.: Norton* (1974).
- [34] Jon M Kleinberg. 1999. Authoritative sources in a hyperlinked environment. *JACM* (1999).
- [35] Erwin Kreyszig. 1979. *Advanced Engineering Mathematics*. John Wiley & Sons.
- [36] Haewoon Kwak, Changhyun Lee, Hosung Park, and Sue Moon. 2010. What is Twitter, a social network or a news media?. In *WWW*.
- [37] Christian Albrekt Larsen. 2013. *The rise and fall of social cohesion: The construction and de-construction of social trust in the US, UK, Sweden and Denmark*. Oxford University Press.
- [38] Jure Leskovec, Daniel Huttenlocher, and Jon Kleinberg. 2010. Predicting positive and negative links in online social networks. In *WWW*.
- [39] Albert J Lott and Bernice E Lott. 1965. Group cohesiveness as interpersonal attraction: a review of relationships with antecedent and consequent variables. *Psychological bulletin* (1965).
- [40] Winter Mason. 2010. Crisis mapping as Collective Problem Solving. *ACM Transactions on Applied Perception* (2010).
- [41] Paolo Massa and Paolo Avesani. 2005. Controversial users demand local trust metrics: An experimental study on epinions.com community. In *National Conference on AI*.
- [42] Paolo Massa, Kasper Souren, Martino Salvetti, and Danilo Tomasoni. 2001. Trustlet, open research on trust metrics. *Scalable Computing: Practice and Experience* (2001).
- [43] Meenakshi Nagarajan, Karthik Gomadam, Amit P Sheth, Ajith Ranabahu, Raghava Mutharaju, and Ashutosh Jadhav. 2009. *Spatio-temporal-thematic analysis of citizen sensor data: Challenges and experiences*.
- [44] Lawrence Page, Sergey Brin, Rajeev Motwani, and Terry Winograd. 1999. The PageRank citation ranking: bringing order to the web. (1999).
- [45] James W Pennebaker, Martha E Francis, and Roger J Booth. 2001. Linguistic inquiry and word count: LIWC 2001. *Mahway: Lawrence Erlbaum Associates* (2001).
- [46] Hemant Purohit, Yiye Ruan, David Fuhry, Srinivasan Parthasarathy, and Amit P Sheth. 2014. On Understanding the Divergence of Online Social Group Discussion. *ICWSM* (2014).
- [47] Gene I Rochlin. 2004. Mind the gap: The growing distance between institutional and technical capabilities in organizations performing critical operations. In *Intelligence and Security Informatics*.
- [48] Daniel M Romero, Wojciech Galuba, Sitaram Asur, and Bernardo A Huberman. 2011. Influence and passivity in social media. In *ECML PKDD*.
- [49] Venu Satuluri and Srinivasan Parthasarathy. 2012. Bayesian locality sensitive hashing for fast similarity search. *VLDB Endowment* (2012).
- [50] Piotr Sztompka. 1999. Trust: A sociological theory. In *Cambridge University Press*.
- [51] Henri Tajfel. 2010. Social identity and intergroup relations. In *Cambridge University Press*.
- [52] Jiliang Tang, Huiji Gao, Xia Hu, and Huan Liu. 2013. Exploiting homophily effect for trust prediction. In *WSDM*.
- [53] Jiliang Tang, Huiji Gao, and Huan Liu. 2012. mTrust: discerning multi-faceted trust in a connected world. In *WSDM*.
- [54] Jiliang Tang and Huan Liu. 2015. *Trust in Social Media: Synthesis Lectures on Information Security, Privacy, and Trust*. Morgan & Claypool Publishers.
- [55] Mike Thelwall, Kevan Buckley, and Georgios Paltoglou. 2012. Sentiment strength detection for the social web. *JASIST* (2012).
- [56] Sarah Vieweg, Amanda L Hughes, Kate Starbird, and Leysia Palen. 2010. Microblogging during two natural hazards events: what Twitter may contribute to situational awareness. In *SIGCHI*.
- [57] Jianshu Weng, Ee-Peng Lim, Jing Jiang, and Qi He. 2010. Twitterank: finding topic-sensitive influential twitterers. In *WSDM*.
- [58] Baoning Wu, Vinay Goel, and Brian D Davison. 2006. Topical trustrank: Using topicality to combat web spam. In *WWW*.
- [59] Wei Xu, Xin Liu, and Yihong Gong. 2003. Document clustering based on non-negative matrix factorization. In *SIGIR*.
- [60] Cai-Nicolas Ziegler and Jennifer Golbeck. 2007. Investigating interactions of trust and interest similarity. *Decision support systems* (2007).

Nikhita Vedula, Srinivasan Parthasarathy, and Valerie L. Shalin