

# On Computational Approaches to Trust Evaluation in Large-Scale Social Networks

Shahriar Etemadi Tajbakhsh and Gaojie Chen and Justin Coon

Department of Engineering Science  
University of Oxford  
Oxford, UK

Email: {shahriar.etemaditajbakhsh, gaojie.chen, justin.coon}@eng.ox.ac.uk

**Abstract**—In this paper, we consider the problem of evaluating trust between individuals in social networks. The previously introduced *three-valued subjective logic* (3VSL) provides a set of useful tools in measuring interpersonal trust in social human networks. However, the number of required operations for such measurements grows exponentially with the size of network. Moreover, the correlations between different paths connecting the two individuals caused by common edges are not considered. In this paper, we show that the operators in 3VSL can still be used to give a lower-bound on trust even if such correlations are taken into account. We introduce a low complexity scalable algorithm to obtain this lower-bound. The numerical experiment results are represented and compared with the 3VSL.

**Keywords**—Trust, Social Networks, Correlation Inequalities.

## I. INTRODUCTION

Uncertainty in predicting others' behaviors naturally exists in many networks including human social networks and communication networks. Rationally individuals should take the level of uncertainty into account in making decisions in their interactions with others. If an individual A trusts B, it means that with high probability A can expect B would act as desired by A. Therefore less caution is required in dealing with B. Trust is usually built based on previous observations of the behaviors of a given agent [1, 2]. For instance, in many online markets, the feedback from previous customers about the quality of service provided by different sellers is given. Hence the users make their decisions based on these ratings. This is, to a very good extent, similar to social human networks where individuals further trust those ones with whom they have had a better experience (based on their behavior in the past).

It should be noted that trust as a general term is a complicated psychological concept and hardly measurable. However, in practical engineering systems such as online social networks or e-commerce, a mathematical model of trust is highly desirable in decision making. As discussed earlier, such a model can rely on the previous observations from the behaviors of an agent. For instance, if we observe  $r$  instances of *good* behavior and  $s$  instances of *bad* behavior, we can expect that with probability  $\frac{r}{r+s}$  we observe a good behavior from the person in her next action. Using this intuition, in [1] the *reputation* of an agent, i.e. the probability distribution

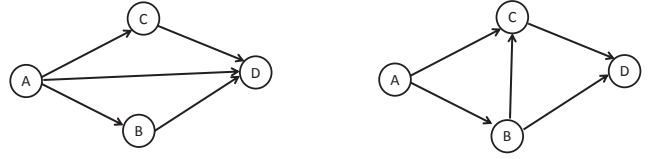


Fig. 1: Series-parallel topology (left) vs. bridge topology (right)

of the probability of good behavior<sup>1</sup> is modeled with the beta distribution with parameters obtained from the previous observations. Similar studies extend the idea of evidence-based trust, for instance [3] models trust as the certainty in predicting the future actions of an agent based on the precedent evidences. It should be noted that recommendation-based trust can be prone to feedbacks by malicious nodes. A robust method of trust analysis against such events is proposed in [4].

Trust, in networks, is however more complicated. In a network of agents, in similarity to human social networks, formation of trust is not only based on agent-to-agent contact through a direct contact (acquaintance), but also affected by indirect contacts via intermediate agents. Trust in multiple hops have a transitive nature, however it is discounted from one hop to another depending how much the two sides of a hop trust in each other. For instance if A trusts B with probability  $p_{AB} = 0.8$  and B trusts C with probability  $p_{BC} = 0.8$ , then A is expected to trust C with probability  $p_{AC} = p_{AB}p_{BC} = 0.64$ , given that the observations of A from B and B from C have been independent. Extending trust to complex networks and how the opinions of different nodes should be propagated across the network has been studied in [2, 5–8], in [9] in semantic web and [10] in wireless networks.

Distributed recommendations as a practical model for trust were discussed and suggested in [2] for online networks. Using the mentioned reputation based models, some approximations for trust probability between individuals are given in [5, 11]. However, these methods are based on the assumption that the topology of the underlying graph of the

<sup>1</sup>This can be a confusing terminology. Here, the probability that good behavior occurs is, itself, a random variable. Hence, it has a distribution just like any other random variable.

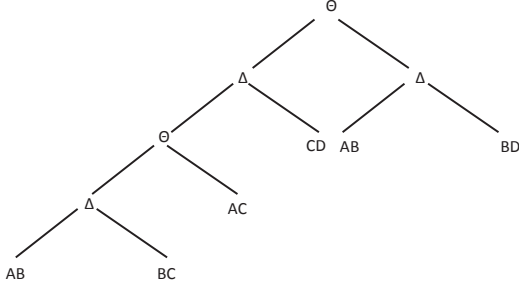


Fig. 2: Tree decomposition of the bridge topology in Fig. 1

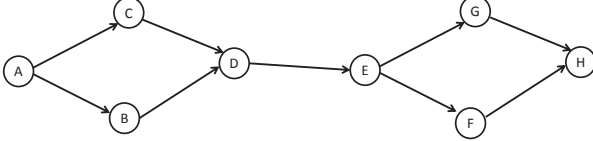


Fig. 3: Two paths  $ABDEGH$  and  $ACDEFH$  are probabilistically dependent.

network only consists of *series* or *parallel* connections. In real social networks the network graph is very likely to be more complicated. For instance, it may include bridge connections as illustrated in Fig. 1. In this case the network cannot be decomposed to only parallel or series connections. In [8], the three-valued subjective logic (3VSL) is introduced and based on that, an algorithm is proposed to measure the trust between two nodes in more complex networks such as the mentioned bridge network topology. In the 3VSL, a quadruple of belief (trust), disbelief (distrust)<sup>2</sup>, *posteriori* uncertainty and *a-priori* uncertainty rates (to be formally defined later) is associated with each pair of trustor  $i$  and trustee  $j$ . We denote this quadruple by  $\omega_{ij} = (b, d, n, e)$ , which is called an *opinion*. Then an equivalent binary decomposition tree of the network directed graph is formed (see Fig. 2) and the two operators *combination* (denoted by  $\Theta$ ) and *discounting* (denoted by  $\Delta$ ) are applied to parallel and series connections, respectively. These operators will be later described and also derived for a more general case of multiple connections. However, it should be briefly noted that in the parallel connections the trustor is receiving multiple opinions from different sources and therefore the combination operator combines all these observations together. In the series connection an opinion about a node  $j$  is discounted while it is transferred through an intermediate node  $k$  to node  $i$ , depending on how much  $i$  trusts in the opinion of  $k$ .

The 3VSL gives a deeper insight about trust propagation through networks. However, there are two main challenges in using the 3VSL which are addressed in this paper and briefly discussed as follows.

- As we will see in Section III, the combination operator in [8] is established based on the assumption of probabilistic independence between parallel connections. However, even if the opinions between different

pairs are formed based on independent observations, opinions coming from paths with common edges are not independent. For instance, in Fig. 3, the two paths  $ABDEGH$  and  $ACDEGH$  are not independent because of sharing the edge  $DE$  in the graph. In this paper, we revisit the theoretical background on the combination of opinions in networks and use the Fortuin-Kasteleyn-Ginibre (FKG) correlation inequality [12, 13] to show that the combination operator in [8] is a lower bound on the probability of trust (or distrust) for parallel connections. The FKG inequality has been widely used in percolation theory [14] and in network modeling [15, 16].

- The number of required operations in the binary tree decompositions grows exponentially with the size of the network. Therefore, it is computationally costly to scale the algorithm to large scale networks. In this paper, we propose a low-complexity algorithm which provides a lower bound on the probability of trust and disbelief with an order  $O(N^3)$  of required operations.

The rest of this paper is organized as follows. The system model and mathematical formulation of the opinions quadruples is provided in Section II. In Section III we prove that the combination operator gives the lower bound for the probabilities of belief and disbelief. The low complexity algorithm for measuring trust in complex networks is given in Section IV. Numerical experiments are represented in Section V and the paper is concluded in Section VI.

## II. SYSTEM MODEL

As mentioned earlier, trust between two individuals in online social networks can be mathematically expressed as the expected probability of observing a desired action from a trustee by a trustor based on previous observations. The system model used in this paper is mainly adopted from the three-valued subject logic introduced in [8]. In this model, we denote the number of desired observations (e.g. positive feedback in an online market) by  $r$ , the number of undesired behaviours (e.g. negative feedback) by  $s$  and neutral observations by  $o$ . The opinion of a node  $i$  about node  $j$  is denoted by  $\omega_{ij}$  and is defined as follows.

$$\omega_{ij} = (b_{ij}, d_{ij}, n_{ij}, e_{ij})$$

$$b_{ij} + d_{ij} + n_{ij} + e_{ij} = 1$$

where  $b_{ij}$ ,  $d_{ij}$ ,  $n_{ij}$  and  $e_{ij}$  are the belief (trust), disbelief, *posteriori* uncertainty and *priori* uncertainty rates. In the absence of any observation, *priori* uncertainty is the probability of trustworthiness, distrust or neutrality. In the following we state the relationship between the mentioned rates, observations (feedback) and the probabilities. The rates

<sup>2</sup>In this paper we use the terms trust and belief interchangeably. Also we use the terms disbelief and distrust interchangeably.

in the opinion quadruple are obtained as follows.

$$\begin{aligned} b_{ij} &= \frac{r}{r+s+o+3} \\ d_{ij} &= \frac{s}{r+s+o+3} \\ n_{ij} &= \frac{o}{r+s+o+3} \\ e_{ij} &= \frac{3}{r+s+o+3} \end{aligned} \quad (1)$$

In the absence of any feedback,  $e_{ij} = 1$ , which is translated to absolute a-priori uncertainty (this results in equal probabilities of trust, distrust and posteriori uncertainty as we will see in (2), and that is how the summation with 3 in the denominators in (1) is justified).

If we run a set of trials with two possible outcomes (e.g. head and tails), and we observe  $r$  heads and  $s$  tails, the probability distribution of  $p$  as the probability of head follows the Beta distribution. In other words, the probability  $p$  itself is considered as a random variable. In the reputation based model introduced in [1], only positive and negative feedbacks are considered and therefore the expected value of the Beta distribution is considered as the probability of trust (or distrust). In the 3VSL there are three possible outcomes, i.e. trust, disbelief and neutral. Therefore, instead of the Beta distribution, the trinomial Dirichlet distribution is used which can be considered as the extension of the Beta distribution to the experiments with more than two possible outcomes. The pdf of the Dirichlet distribution is as follows.

$$f(P_b, P_d | \alpha, \beta, \gamma) = \frac{\Gamma(\alpha + \beta + \gamma)}{\Gamma(\alpha)\Gamma(\beta)\Gamma(\gamma)} P_b^{\alpha-1} P_d^{\beta-1} P_n^{\gamma-1}$$

where  $\alpha$ ,  $\beta$  and  $\gamma$  are the parameters of the Dirichlet distribution and  $\Gamma(\cdot)$  is the Gamma function. Also  $P_b$  and  $P_d$  are the probabilities of trust and distrust, respectively. Based on the definition of the mentioned distribution the expected probability of belief, distrust and uncertainty is related to the observations and obtained as follows.

$$\begin{aligned} E(P_b) &= \frac{\alpha}{\alpha + \beta + \gamma} = \frac{r+1}{r+s+o+3} = b_{ij} + \frac{1}{3}e_{ij} \\ E(P_d) &= \frac{\beta}{\alpha + \beta + \gamma} = \frac{s+1}{r+s+o+3} = d_{ij} + \frac{1}{3}e_{ij} \\ E(1 - P_b - P_d) &= \frac{\gamma}{\alpha + \beta + \gamma} = \frac{o+1}{r+s+o+3} = n_{ij} + \frac{1}{3}e_{ij} \end{aligned} \quad (2)$$

Therefore, the probability space is split into three parts; trust, distrust and the remainder is uncertainty. In this paper, we assume the topology of the network is defined according to the adjacency matrix  $\mathbf{A}$ , where  $\mathbf{A}_{ij} = 1$  if nodes  $i$  and  $j$  are connected to each other, i.e. they can directly communicate with each other and  $\mathbf{A}_{ij} = 0$  otherwise. We assume that  $\mathbf{A}_{ij} = 0$  is translated to  $\omega_{ij} = (0, 0, 0, 1)$ , i.e.  $e_{ij} = 1$ . The physical meaning of the setting is that if two nodes cannot communicate, they are entirely uncertain about the trustworthiness of each other (through a direct contact). As we will see later, this assumption simplifies designing the low complexity algorithm.

### III. LOWER BOUND

In [8], the *combination* operator is introduced to combine the trust probabilities of parallel paths. Here we derive the operator for multiple paths. However, the fundamental contribution of this section is to show that the derived operator gives a lower bound on the probabilities of trust and distrust. As discussed earlier and illustrated in Fig. 3, the correlation between paths with common edges is ignored in [8]. The impact of this correlation may be different from one network to another depending on their topologies. However, from a theoretical perspective it is important to recognize this correlation and understand how it affects the trust. It should be noted that when two paths share an edge, it means that both paths are influenced by identical observations over the common edge.

To obtain the lower bound we rely on FKG correlation inequality [12, 13]. This inequality gives a lower bound on the probability of the intersection of *monotonically increasing* (or decreasing) events (or families of events). An event  $A$  is said to be increasing if the indicator function is an increasing variable, i.e.  $\mathbf{1}_A(\delta) \geq \mathbf{1}_A(\delta')$  whenever  $\delta \geq \delta'$ . For instance, existence of a path between two specific nodes through a given set of nodes is an increasing event. If  $\mathcal{A}$  and  $\mathcal{B}$  are two families of monotonically increasing events, FKG correlation inequality states that,

$$P(\mathcal{A} \cap \mathcal{B}) \geq P(\mathcal{A})P(\mathcal{B}) \quad (3)$$

In percolation theory, this theorem is fundamental to understanding path formation in random graphs. Belief and distrust are both monotonically increasing functions. For instance, consider four nodes  $A, B, C, D$  which are connected in tandem ( $A \rightarrow B \rightarrow C \rightarrow D$ ). If we know that  $A$  trusts  $D$  via this path, we conclude that  $B$  must trust  $C$ . Similarly if we know that  $A$  distrusts  $D$  then  $B$  must trust  $C$  and  $C$  distrusts  $D$  (hence  $C$ 's disbelief in  $D$  could be believed by  $B$  as  $B$  trusts in  $C$ ). Similarly  $A$  should trust  $B$  to believe in the discounted disbelief of  $B$  about  $D$ .

Now suppose that there exists  $M$  paths from node  $i$  to node  $j$ . Since each of these paths is a monotonically increasing event, using FKG the combined probability density function of these paths is obtained as stated in the following Lemma.

**Lemma 1.** *For  $M$  parallel paths between any two nodes in a graph we have:*

$$\begin{aligned} g(P_b, P_d) &\geq f(P_b, P_d) \left( \sum_{m=1}^M \alpha_m - M + 1, \sum_{m=1}^M \beta_m - M + 1, \right. \\ &\quad \left. \sum_{m=1}^M \gamma_m - M + 1 \right) \end{aligned} \quad (4)$$

where  $g(P_b, P_d)$  is the combined pdf of trust and distrust and  $f(\cdot)$  is the trinomial Dirichlet distribution with parameters  $\sum_{m=1}^M \alpha_m - M + 1$ ,  $\sum_{m=1}^M \beta_m - M + 1$  and  $\sum_{m=1}^M \gamma_m - M + 1$ .

*Proof:* The r.h.s Dirichlet distribution  $f$  is actually the product of the distributions of trust (or distrust) on the  $M$  paths. Therefore, the inequality is immediately resulted from (3). If the paths are mutually edge-disjoint, the equality holds. ■

In the following, we apply lemma 1 to derive the inequalities of the Proposition 2. These inequalities will be used in Section IV to obtain a lower bound on the probabilities of trust and distrust between any two given nodes.

By substituting the values of  $\alpha_m$ , we have,

$$E(P_b) \geq \frac{\left(\sum_{m=1}^M \alpha_m\right) - M + 1}{\left(\sum_{m=1}^M \alpha_m + \beta_m + \gamma_m\right) - 3M + 3} = \frac{\left(\sum_{m=1}^M r_m\right) + 1}{\left(\sum_{m=1}^M r_m + s_m + o_m\right) + 3} \quad (5)$$

where  $\alpha_m - 1$  has been replaced by  $r_m$  (trust rate associated with path  $m$ ) according to the definition of the Dirichlet distribution. By substituting  $r_m + s_m + o_m = 3(\frac{1}{e_m} - 1)$  and  $r_m = 3\frac{b_m}{e_m}$  in (5) we have

$$E(P_b) \geq \frac{\sum_{m=1}^M b_m \prod_{\ell=1, \ell \neq m}^M e_\ell + \prod_{m=1}^M e_m}{\sum_{m=1}^M \prod_{\ell=1, \ell \neq m}^M e_m - (M-1) \prod_{m=1}^M e_m} \quad (6)$$

Therefore, by combining (2) and (6) we have:

$$b = \frac{\sum_{m=1}^M b_m \prod_{\ell=1, \ell \neq m}^M e_\ell}{\sum_{m=1}^M \prod_{\ell=1, \ell \neq m}^M e_m - (M-1) \prod_{m=1}^M e_m} \quad (7)$$

and

$$e = \frac{\prod_{m=1}^M e_m}{\sum_{m=1}^M \prod_{\ell=1, \ell \neq m}^M e_m - (M-1) \prod_{m=1}^M e_m} \quad (8)$$

Similarly  $d$  and  $n$  are obtained as follows.

$$d = \frac{\sum_{m=1}^M d_m \prod_{\ell=1, \ell \neq m}^M e_\ell}{\sum_{m=1}^M \prod_{\ell=1, \ell \neq m}^M e_m - (M-1) \prod_{m=1}^M e_m} \quad (9)$$

and

$$n = \frac{\sum_{m=1}^M n_m \prod_{\ell=1, \ell \neq m}^M e_\ell}{\sum_{m=1}^M \prod_{\ell=1, \ell \neq m}^M e_m - (M-1) \prod_{m=1}^M e_m} \quad (10)$$

The collection of (7), (9), (10) and (8) is called the combination operator and is denoted by  $\Theta(\omega_1, \dots, \omega_M)$ . It should be noted that the similar procedure can be applied to the probability  $P_d$  (probability of distrust) to obtain its lower-bound. Hence, the following proposition is resulted.

**Proposition 2.** *The following inequalities hold for  $P_b$  and  $P_d$ .*

$$\begin{aligned} E(P_b) &\geq b + \frac{1}{3}e \\ E(P_d) &\geq d + \frac{1}{3}e \end{aligned} \quad (11)$$

Therefore, the certainty part including trust and distrust is lower bounded by the above equations and hence the uncertainty is upper-bounded by  $n + \frac{1}{3}e$ .

#### IV. ALGORITHM

In this section, we exploit the lower bound discussed in Section III and incorporate it to an iterative algorithm to obtain a lower bound on the probabilities of trust and distrust between each pair of nodes in the network. As discussed earlier, the combination operator is applied to parallel connections. For series connections, the discounting operator is introduced in [8] and comes as follows.

$$\Delta(\omega_{ij}, \omega_{kj}) = \begin{cases} b_{ij} = b_{ik} b_{kj} \\ d_{ij} = b_{ik} d_{kj} \\ n_{ij} = 1 - b_{ij} - d_{ij} - e_{kj} \\ e_{ij} = e_{kj} \end{cases} \quad (12)$$

The algorithm begins with the initial values of the opinions and applies the discounting operator to all the paths of maximum length 2 between each pair of nodes  $i$  and  $j$ , and then the opinions on these paths are combined by the combination operator (see Fig. 4). The opinion on each pair  $i$  and  $j$  is updated to the new opinion obtained from the mentioned calculation and the next iteration is run for the updated values until the algorithm is halted once it reaches the required number of iterations  $T$ . As mentioned earlier, for those nodes  $i$  and  $j$  which are not connected in the the graph topology, the initial value of the opinion of  $i$  about  $j$  is set to be  $(0, 0, 0, 1)$  (i.e.  $e_{ij} = 1$ ). The discounting operator can be nested in the combination algorithm for these parallel paths. For instance, the final operator for the trust probability over these paths of maximum length 2 on a graph with  $N$  nodes would be obtained as follows.

$$\Psi(i, j) = \Theta(\omega_{ij}, \Delta(\omega_{i1}, \omega_{1j}), \Delta(\omega_{i2}, \omega_{2j}), \dots, \Delta(\omega_{iN}, \omega_{Nj})) \quad (13)$$

It should be noted that since the discounting gives the exact values of the opinions on series connections, the opinions on trust and distrust obtained from the operator  $\Psi$  are lower bounds. The algorithm is summarized in Algorithm 1.

The main contribution of the proposed algorithm is in its dramatically lower computational complexity in comparison to the binary decision tree based algorithm in [8]. As it can be observed from the algorithm and the used operators, the order of the complexity of the algorithm is of  $\mathcal{O}(N^3)$ , as the number of operations in each combining operation is of  $\mathcal{O}(N)$  and these operations should be performed for  $\mathcal{O}(N^2)$  edges across the network. Whereas the size of the binary tree grows exponentially in edge dense network. In the worst case scenario, in a clique graph (a graph in which there exists an edge between any two vertices), the entire set of possible paths of length 1 to length  $N - 2$  should be considered. Therefore, it would be computationally costly to be deployed in large-scale networks.

The low complexity of the algorithm comes from the fact that the calculations are not performed on individual pairs. Instead the collective calculations on paths of at most length 2 on all the pairs in the graph are then used in the next



**Algorithm 1** Trust Assessment

---

```

1: for  $t = 1 : T$  do
2:   for  $i = 1 : N$  do
3:     for  $j = 1 : N$  do
4:        $\omega_{ij} \leftarrow \Psi(i, j)$ 

```

---

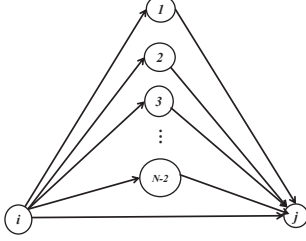


Fig. 4: At each iteration the algorithm is performed on paths of at most length 2 between each pair of nodes  $i$  and  $j$

iteration for all pairs. Therefore, the influence of nodes on others' opinions is spread at a faster speed. For instance in the first iteration, the opinion of each node  $i$  about a node  $j$  is influenced by all the nodes within a distance of 1 hop from  $i$ . In the next iteration, all the paths of at most length 4 participate in the formation of  $i$ 's opinion about  $j$ . This is due to the fact that in the second round all the opinions are the results of two hop calculations from the previous round and hence any two hop connection might be influenced by at most 4 hops from  $i$  to  $j$ . After  $T$  iterations, paths of length  $2^T$  have influenced all the opinions. Since the social networks have a small diameter [17], the number of iterations required to reach from each node to another is quite small (even though the network is large-scale as  $N$  is large). For instance, if we take the so-called six degrees of separation into account, at most  $T = 4$  would be sufficient to reflect the opinions of the entire network about an individual.

## V. NUMERICAL EXPERIMENTS

In this section, we provide some numerical results to firstly compare the 3VSL and the algorithm proposed in this paper and then represent the impact of network parameters on formation of trust between individual nodes. In the first experiment we have generated two networks with different parameters. Other than the size of the network denoted by  $N$  (number of nodes), we assume that with probability  $q$ , a node is connected to another (the graph is directional). Therefore,  $q = 1$  means that the network is a clique graph where there is an edge between any two vertices. To generate the initial values for the opinions between the nodes in the network, we assume that with probability  $\rho$  a node is trustworthy and the trust rate in that node is  $b = 0.7 + 0.3r$  on the incoming edges where  $r$  is a uniformly chosen random number between 0 and 1. We call  $\rho$  the probability of goodness. The reason for this type of modeling is to resemble the real world where the trustworthy nodes usually represent a similar behavior towards different nodes. With probability  $1 - \rho$ , a node is not trustworthy and hence the distrust rate in that node is  $d = 0.7 + 0.3r$  on each incoming edge. Also in the proposed

Parameters	3VSL	Prop. Algorithm	CPU1	CPU2
$N = 10$ , $L = 8$ , $T = 4$ , $q = 1$ , $\rho = 1$	$b = 0.28$ , $d = 0.03$ , $n = 0.67$	$b = 0.20$ , $d = 0.02$ , $n = 0.76$	35.45	0.0156
$N = 25$ , $L = 4$ , $T = 3$ , $q = 1$ , $\rho = 1$	$b = 0.50$ , $d \approx 0$ , $n = 0.49$	$b = 0.43$ , $d \approx 0$ , $n = 0.56$	355.9	0.06

TABLE I: Two networks: comparing the algorithm in [8] and the proposed algorithm

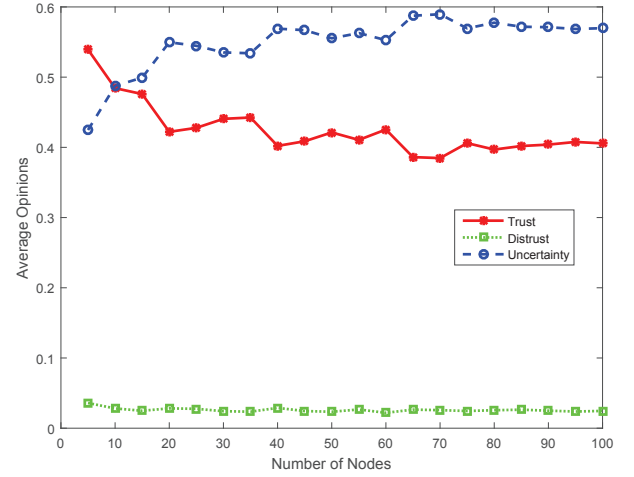


Fig. 5: Trust and distrust versus the size of network

algorithm we assume we have  $T$  iterations of the algorithm and for the 3VSL we do not consider paths of length more than  $L$  (as it would be computationally hard to take large paths into account because of the exponential growth in the number of such paths). We have also measured the CPU time to compare the computational complexity of the two algorithms (CPU1 for 3VSL and CPU2 for the proposed algorithm in Table I). As it can be seen from the table, the computational complexity of the algorithm in [8] is dramatically higher than the proposed algorithm in this paper. We have selected a random pair of nodes and the opinions on the edge connecting the pair is reported here. The results are represented in Table I.

As it can be observed from the table, when  $T$  and  $L$  are in the range where comparison is fair between two algorithm, e.g.  $T = 3$  (which means nodes within 8 hops have had influence) and  $L = 4$ , the opinions resulted from the two algorithms are not far from each other. It is also important to remember that the results from our algorithm and the 3VSL are both lower bounds on trust and distrust.

We further considered the impact of the size of the network on the opinions. Here we have measured the average opinions across the network on all of the edges. Networks

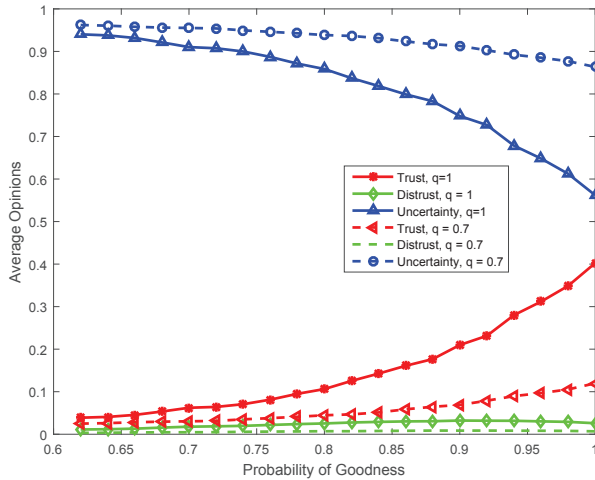


Fig. 6: Impact of the probability of goodness and connectivity of the network on trust and distrust

from size  $N = 5$  to  $N = 100$  have been compared in Fig. 5, where  $q = 1$  and  $\rho = 1$ . As it can be observed from the figure, trust declines relatively rapidly in the smaller networks with the growth of the size of network but remains nearly constant in the larger networks. In Fig. 6 the impact of the probability of goodness  $\rho$  and also the probability of connectivity  $q$  has been shown. As it is expected, by increasing the fraction of good nodes from  $\rho = 0.6$  to  $\rho = 1$ , the trust increases and hence the uncertainty decreases. Distrust in such networks with a large fraction of trustworthy nodes ( $\rho > 0.5$ ) is small and remains nearly constant.

## VI. CONCLUSION

Evidence based trust and reputation based models of measuring trust have been studied in the literature. Extending the concept to complex networks is however, relatively new. In this paper, we revisited the theoretical foundation of a previous study on trust in social networks and we proved that the proper operators can provide a lower bound on the probabilities of trust and distrust. Moreover, we proposed an algorithm to obtain a lower bound on trust and distrust which enables us to study trust in large scale social networks. Although the focus of this paper is mainly on the microscopic level measurements of trust (between individual nodes), it can be a strong basis for a macroscopic level study in future.

## ACKNOWLEDGMENT

This work was supported in part by EPSRC grant number EP/N002350/1 (Spatially Embedded Networks).

## REFERENCES

- [1] B. E. Commerce, A. Jøsang, and R. Ismail, "The beta reputation system," in *Proceedings of the 15th Bled Electronic Commerce Conference*. Citeseer, 2002.
- [2] A. Abdul-Rahman and S. Hailes, "A distributed trust model," in *Proceedings of the 1997 workshop on New security paradigms*. ACM, 1998, pp. 48–60.

- [3] Y. Wang and M. P. Singh, "Evidence-based trust: A mathematical model geared for multiagent systems," *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, vol. 5, no. 4, 2010.
- [4] X. Wang, L. Liu, and J. Su, "Rlm: A general model for trust representation and aggregation," *IEEE Transactions on Services Computing*, vol. 5, no. 1, pp. 131–143, 2012.
- [5] C.-W. Hang, Y. Wang, and M. P. Singh, "Operators for propagating trust and their evaluation in social networks," in *Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems-Volume 2*, 2009, pp. 1025–1032.
- [6] Y. Wang, C.-W. Hang, and M. P. Singh, "A probabilistic approach for maintaining trust based on evidence," *Journal of Artificial Intelligence Research*, vol. 40, no. 1, pp. 221–267, 2011.
- [7] Y. Wang and M. P. Singh, "Trust representation and aggregation in a distributed agent system," in *AAAI*, vol. 6, 2006, pp. 1425–1430.
- [8] G. Liu, Q. Yang, H. Wang, X. Lin, and M. P. Wittie, "Assessment of multi-hop interpersonal trust in social networks by three-valued subjective logic," in *IEEE Conference on Computer Communications (INFOCOM)*, 2014.
- [9] M. Richardson, R. Agrawal, and P. Domingos, "Trust management for the semantic web," in *International semantic Web conference*. Springer, 2003, pp. 351–368.
- [10] J. P. Coon, "Modelling trust in random wireless networks," in *The 11th International Symposium on Wireless Communications Systems (ISWCS)*, 2014, pp. 976–981.
- [11] A. Jøsang and T. Bhuiyan, "Optimal trust network analysis with subjective logic," in *2008 Second International Conference on Emerging Security Information, Systems and Technologies*. IEEE, 2008, pp. 179–184.
- [12] C. M. Fortuin, P. W. Kasteleyn, and J. Ginibre, "Correlation inequalities on some partially ordered sets," *Communications in Mathematical Physics*, vol. 22, no. 2, pp. 89–103, 1971.
- [13] T. E. Harris, "A lower bound for the critical probability in a certain percolation process," in *Proc. Cambridge Philos. Soc*, vol. 56. Cambridge Univ Press, 1960, pp. 13–20.
- [14] H. Kesten, *Percolation theory for mathematicians*. Springer, 1982.
- [15] S. Zhao and X. Wang, "Node density and delay in large-scale wireless networks with unreliable links," *IEEE/ACM Transactions on Networking*, vol. 22, no. 4, pp. 1150–1163, 2014.
- [16] W. Ren, Q. Zhao, and A. Swami, "On the connectivity and multihop delay of ad hoc cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 4, pp. 805–818, 2011.
- [17] D. J. Watts and S. H. Strogatz, "Collective dynamics of small-world networks," *nature*, vol. 393, no. 6684, pp. 440–442, 1998.