Controversy-aware Hybrid Trust Inference in Online Social Networks

Paolo Zicari, Roberto Interdonato, Andrea Tagarelli, Sergio Greco
DIMES, Università della Calabria, Italy

***Abstract*—Social interactions assume a central role in everyday life of people strongly connected through online social networks and web communities. Trust can be used as a filter to the increasing flow of information, experiences and opinions exchanged among users. In the absence of direct relations, trust inference algorithms can be exploited in order to estimate missing trust values. However, controversial situations can easily arise from the subjectivity of trust opinions, when the lack of agreement leads to ambiguity and uncertainty in the inferred trust. In this work, we propose a novel trust inference algorithm, named *TrustZic*, which aims at improving the performance of trust inference in controversial conditions by combining local and global trust aspects. The proposed approach is based on the use of global reputation values as node weights biasing a local trust inference process. Experimental evaluation has shown the significance of our approach and its effectiveness in supporting trust decisions in critical situations characterized by a high level of controversy.**

I. Introduction

Nowadays, online social networks (OSNs) and web communities have imposed their central role in the life of millions of people as the preferred mean to share information, experiences and opinions through continuous interactions. Social interactions happen without any geographical or temporal limit, and the information that anyone shares can easily reach a vast crowd, mainly composed by people which does not have a real direct knowledge of each other (e.g., unlike what usually happens in off-line small communities). In this scenario, it becomes necessary to introduce a mechanism for validating and filtering content, discerning the veracity of the information and selecting the appropriate people with whom to share opinions and preferences. A popular way to address this problem is to take into account the concept of *trust*, i.e., modeling information about how much trustworthy each user considers the other ones. OSNs containing information about trust relationships between pair of users are generally referred to as *trust networks*.

A large body of work exists which focuses on the definition of trust inference algorithms, i.e., methods capable of inferring the level of trust between users not directly connected to each other [1], [2]. Trust inference algorithms are typically classified into two main categories: *local* and *global* methods. Local methods infer the trust from a source node to a sink (i.e., target) node by modeling the trust propagation flow across the paths connecting the two nodes. This approach preserves the subjectivity of the trust statements, i.e., inferred trust values for the same target user can be completely different when coming from different source nodes. Conversely, global approaches are based on the calculation of a single trust evaluation for each user, which should reflect the opinion of the entire community; the notion of trust, which in this case can also be referred to as *reputation*, is considered as a global ranking of the users [3], [4], [5].

Controversial situations can easily arise in trust networks because of the discordance between personal (subjective) opinions [6], [7], [8], [9]. These situations may occur when there is no agreement in the trust statements towards a user, leading to interpretation and reliability problems in the trust inference process. Local trust inference approaches have been proved to be more effective in presence of controversial conditions [7].

The aim of this work is to highlight the improvements that can be obtained in this context by combining information coming from both local and global trust aspects in the disambiguation of *controversial* situations, i.e., cases where the trust opinions widely differ from each other, without a strong unanimous consensus. Our key ideas and contributions are the following:

- We analyze several controversial cases, considering the use of both global and local methods to improve performances in terms of error prediction and accuracy.
- We propose a novel trust inference algorithm, namely *TrustZic*, which takes into consideration both local and global trust aspects, i.e., propagating trust evaluations proportionally to the global reputation of the trustor nodes.
- We provide explanatory examples and experimental results in a real dataset, proving the effectiveness and significance of the proposed *TrustZic* in solving controversial situations.

The remainder of the paper is organized as follows. Section II introduces the scenario which motivates our proposal, Section III discusses related works, Section IV introduces the proposed *TrustZic* algorithm, Section V discusses experimental evaluation, and Section VI concludes the work.

II. The motivating scenario

This section introduces a typical scenario that highlights the motivations underneath the proposed research work. Figure 1 shows a simple controversial condition that can happen in a social network context. Paul needs to hire a new employee for his company. After advertising the open position, Paul receives an application from Ken. Unfortunately, Paul does not know anything about Ken, but he is in touch with John and Mark, who had previous work experiences with Ken. Paul

2324-9013/17 $31.00 © 2017 IEEE
DOI 10.1109/Trustcom/BigDataSE/ICESS.2017.291

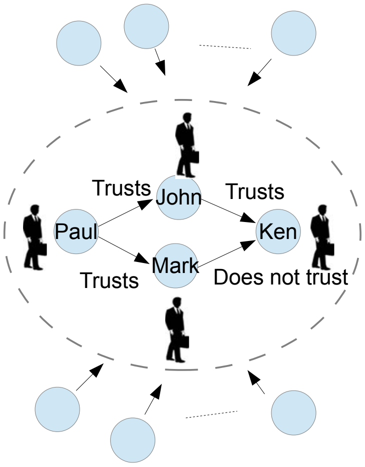

Fig. 1. A typical trust controversy case: it is not possible to infer whether or not Paul should trust Ken.

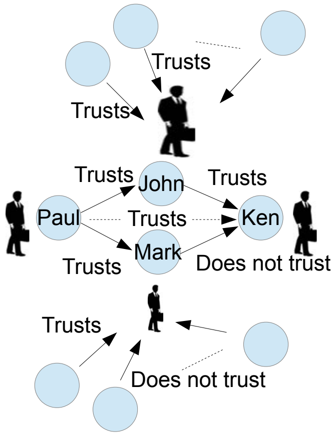

Fig. 2. A controversy case addressed in a global scenario, where the size of the user figures is proportional to their reputation.

is happy because he can now take a decision based on the experiences reported by John and Mark. After asking them, he receives two controversial opinions about Ken. In fact, John recommends Ken as a good choice for filling the job position, while Mark reports negative experiences about the behavior of Ken at work. As Paul has the same consideration of John and Mark, he is unable to take a decision about Ken.

This is a typical situation of trust controversy, where trusted users report contrasting opinions. A reasonable decision about trusting or not a user in such a controversial situation is not possible, since the trusting paths connecting source and target nodes are propagating opposite opinions.

The main idea of our proposed approach to solve this problem is to exploit information from the rest of the trust network in order to find a way for solving the controversial situation. To this purpose, it is necessary to introduce a criterion of discernment. The most natural way to differentiate the reported trust opinions is to give a different weight depending on the reputation of the trustors. In fact, each user has a different influence with respect to the reputation built in the specific context. The reputation influences the way the opinions, suggestions and recommendations are considered.

Figure 2 reports an extended version of the previous example, where the focus is broadened to include more the network. In this case, the global reputation of the nodes can be used to take a reasonable decision about whether Paul should or should not trust Ken. The extended scenario shows that John is trusted by all his in-neighbors, while Mark received both trust and no-trust statements: in this condition it is clear that John has a higher reputation than Mark. After considering the different reputations of John and Mark, Paul decides to take a final resolution about Ken. In fact, Paul finds that the reputation of John is much higher than that of Mark, so he decides to consider the opinion coming from John more reliable, and finally hires Ken. According to the reported considerations, in the proposed approach the reputation will be used as a discerning weighting factor in controversial situations.

III. Related work

A. Trust Inference

A trust network is usually modeled as a directed graph $G = \langle V, E, T \rangle$, consisting of a set V of nodes (users), a set of links (edges) that represent relations between users, and an edge weighting function T modeling the corresponding trust level of the edges.

The trust network is derived directly from a social network when users are requested to rate each others. *Epinions*[1] is a premier consumer reviews platform on the Web based on the recommendation and the trust among the users who review commercial products. In the *Epinions Web of Trust* technology, users can specify their trust in other users for receiving notifications when the latter ones review new products. In [10], the *Friend-Of-A-Friend* (FOAF) project[2] aimed at building a Web of acquaintances, was extended in order to include information of the level of trust on a scale of 1-9 that users can indicate with respect to the people they know.

Whenever there is no information about how much a user rates other users, the trust network can be derived by evaluating trust statements and interactions among users [11], [12], [13]. In [13], an algorithm based on the communication behavior in social communication networks is proposed in order to measure the trust among users. The trust is measured by quantifying the behavior in terms of length and frequency of communications, and propagation of information among users. Experiments were conducted on Twitter, where the mechanism of *retweet* was used for measuring the trust contribution coming from propagation.

The purpose of a generic trust inference algorithm IT is to compute a prediction of the trust from a source node u to a sink node v when there is no direct link between the two

[1] http://www.epinions.com
[2] http://www.foaf-project.org/

nodes, i.e., $(u, v) \notin E$. Obviously, there is no need to calculate a prediction when an explicit trust statement was issued, i.e., $IT(u, v) = T(u, v)$ if $(u, v) \in E$. Several trust inference algorithms have been proposed in literature for prediction purposes with different characteristics and performances. The trust inference algorithms can be classified into two main categories: *global* and *local* methods [14]. Global algorithms compute an overall evaluation, here commonly named *reputation*, for each user of the trust network; thus, the reputation can be considered as the synthesis of the trust evaluations from the entire network with respect to a single user. The well-known *PageRank* [15] can be considered as a basis for the development of global trust methods [3].

Nevertheless, global trust inference methods are not suited to preserve the characteristic of personalization in the subjective expression of an opinion, which can instead be achieved by using local trust inference algorithms. One of the most popular local trust inference algorithms is *TidalTrust* [14], which computes the trust between non-adjacent nodes by considering only shortest paths through trusted neighbors. Another local method is proposed in [16], namely *TISoN* (Trust Inference within online Social Networks). In this case a selection of the trust paths from a source node to a sink node is performed with respect to two criteria: the maximum allowed depth of the path, and the minimum threshold level allowed for the trust edges in the path. Then the inferred trust is computed selecting the *most trustable path*, based on the average of the trust edges in the path, the path variance of the trust edges w.r.t. the average, and a path weight based on its length. As regards other approaches, a detailed survey of trust inference algorithms in literature is presented in [2].

B. Trust Controversy

As trust statements reflect subjective opinions built on personal experiences, it is often the case that users report contrasting and different trust opinions about the same target. When trust statements differ too much from each other, it becomes challenging to derive affordable inferred trust information. The presence of controversial conditions make the trust inference problem more complex to address. Thus, the identification of controversial conditions requires to be explicitly taken into account when dealing with trust networks. The concept of controversy in trust networks has been widely studied in literature [6], [7], [8], [9].

In [6], the controversy is referred to as single users that are trusted and distrusted by many, i.e., without a global agreement as regards their trustworthiness. The level of controversy for a generic user u is defined by two metrics, controversiality level (c_l) and controversiality percentage (c_p) as follows:

$$c_l(u) = \min(\#r_t(u), \#r_d(u)) \tag{1}$$

$$c_p(u) = \frac{\#r_t(u) - \#r_d(u)}{\#r_t(u) + \#r_d(u)} \tag{2}$$

where the received trust ($\#r_t$) and the received distrust ($\#r_d$) represent the number of trust and distrust edges to the node u, respectively.

Controversy was studied by [8] and [17] in the context of recommender systems, where *controversial reviews* are defined as those reviews that receive a variety of high and low scores, reflecting disagreement about reviews. Those studies introduced a measure of controversy in terms of standard deviation σ of the reviews of an item i and the *level of disagreement* α defined as follows:

$$\alpha(\Delta, i) = 1 - \max_{\alpha \in \{1,\dots,m-\Delta+1\}} \left(\frac{\sum_{s=a}^{a+\Delta-1} f_i(s)}{\sum_{s=1}^{m} f_i(s)} \right) \tag{3}$$

where Δ is the level of a discrete rating scale from 1 to m, and $f_i(s)$ is the number of times that the item i received a rating of score s.

In this work, we will use the metric proposed in [9] in order to evaluate the controversy of the trust inferred from a source node A to a generic sink node Z. The main idea is to consider the controversy as the variance among the trust opinions of the predecessors of the source nodes. To this purpose, the mean trust $TM(A, Z)$ is calculated as follows:

$$TM(A, Z) = \frac{\sum_{P_i \in Pred(Z)} IT(A, P_i) \times T(P_i, Z)}{\sum_{P_i \in Pred(Z)} IT(A, P_i)} \tag{4}$$

where $Pred(Z)$ is the set of predecessors of the node Z, IT indicates the inferred trust values and T the original trust weights.

According to Equation 4, the mean trust is the weighted average of the trust values assigned by the predecessors P_i of node Z, where the weights are the inferred trusts from the source node A to the predecessor nodes P_i. As the controversy measure is related to the level of discordance among the different trust opinions reported to the source node through the trust chains up to the sink node, the controversy measure $TC(A, Z)$ is defined as the weighted variance of the inferred trust paths, as reported in the following:

$$TC(A, Z) = \frac{\sum\limits_{P_i \in Pred(Z)} IT(A, P_i) \times (T(P_i, Z) - TM(A, Z))^2}{\sum\limits_{P_i \in Pred(Z)} IT(A, P_i)} \tag{5}$$

The normalized trust controversy measure (NTC), introduced to bring TC into the range $[0, 1]$, can be computed as follows:

$$NTC(A, Z) = \frac{TC(A, Z)}{((Tmax - Tmin)/2)^2} \tag{6}$$

where $Tmin$ and $Tmax$ are the extremes of the trust range.

C. Local vs. Global methods

How global and local methods should be used to solve different trust inference problems was widely explored in [18]. An interesting comparison of local and global trust metrics is reported in [6], where the characteristics of the two approaches are argued in detail. Results on real datasets proved that global methods show intrinsic limit when controversial users (i.e. users judged in different ways by other users) are analyzed, while local methods are more suitable in contexts where opinions are more subjective like in the controversial conditions. The study in [7] showed how local trust metrics outperform global ones when predicting the trustworthiness of users characterized by both trust and distrust evaluations.

The idea of improving the performance of prediction systems by exploiting both global and local trust metrics is not new in literature. An hybrid global-local method was introduced by [19] in the context of service recommendation systems. The scenario depicted in [19] is different from the one discussed in this work, as it considers a recommendation system consisting of different services rated by users integrated with a trust network. The trust network is used to support the computation of the personalized rating prediction $PT(u, s)$ of a service s from a user u as the weighted average reported in Equation 7 of the global $r(s)$ and local $T(u, s)$ rating evaluation of the service s, where w_l and w_r are the weights used for properly tuning the local and global contributions, respectively:

$$PT(u,s) = \frac{r(s) \times w_r + T(u,s) \times w_l}{w_r + w_l} \tag{7}$$

The promising results obtained by exploiting both global and local perspectives in recommendation systems have encouraged us to investigate how combining the two approaches can be beneficial for improving the performance of trust inference algorithms in controversial conditions.

IV. The TrustZic algorithm

The proposed trust inference method, namely *TrustZic*, aims at solving problems rising when trying to infer trust values in controversial cases, by exploiting global and local trust information in a combined solution. In the proposed approach, the level of trust inferred from the source to the sink will still be personalized because it depends on the propagation of trust along the paths between the source and the sink across the trust graph. Nevertheless, the nodes in the traversed paths are not equally considered, but they exert a different bias on the trust propagation, i.e., proportional to their reputation which is obtained by applying a global trust method.

Figure 3 shows the main steps of the *TrustZic* approach: in the first step a global ranking is calculated from the trust graph in order to get a reputation value $r(i)$ for each node i. The *trust-reputation network* is obtained from the trust network by adding the reputation information on the nodes. In the second step, the trust between nodes not directly connected in the trust network is inferred. The trust inference method propagates the trust from the source node to the sink through the trust paths weighted based upon the reputation of each node traversed across the path. The resulting trust inference network is a complete graph in which nodes are connected by trust relations (solid edges) or inferred trust relations (dashed edges). In the following, we will give detailed information on how we perform these steps.

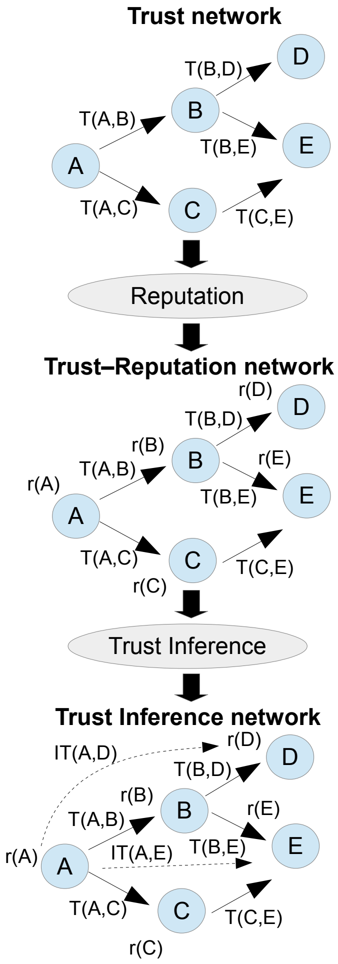

Fig. 3. The fundamental steps of the TrustZic algorithm.

Step 1: computation of the global trust values. A *PageRank*-like algorithm is here used to implement the first step of the proposed method (i.e., obtaining the global ranking of all the nodes in the network). The stochastic matrix M is obtained as the transpose and normalized version of the trust matrix T, as shown in (8).

$$M[i,j] = \frac{T[j,i]}{\sum\limits_{k \in adj(j)} T[j,k]} \tag{8}$$

The vector r of reputations for all the N nodes is calculated as in (9), where α is a smoothing factor (by default set to 0.85) and p is the column vector with the initial reputation value (by default $p = \mathbf{1}$, i.e., the column vector of ones).

$$r = \alpha M r + \frac{1-\alpha}{N} p \tag{9}$$

We then adopt the final PageRank solution (i.e., vector of the stationary distribution of PageRank scores at convergence) to assign reputation values to the nodes in the network. However, this can be thought as a general workflow, where different global ranking methods can be used in theory at this step.

Step 2: local trust inference propagation. The second step consists in propagating the trust from a source node to a sink node by taking into consideration not only the trust T but also the reputation r. The inferred trust $IT(i,j)$ from the source node i to the sink node j is computed as reported in (10), where $d \in (0,1]$ is the decay trust factor, introduced for modeling the fact that the trust generally decreases when increasing the distance from the source node.

$$IT(i,j) = \begin{cases} T(i,j) \text{ if there is a direct trust} \\ \frac{\sum\limits_{k \in neighbor(i)} r(k) \times d \times T(i,k) \times IT(k,j)}{\sum\limits_{k \in neighbour(i)} r(k) \times T(i,k)} \text{ otherwise} \end{cases} \tag{10}$$

In order to disambiguate controversy, trust is propagated from the source node through all the different paths reaching the sink node, without excluding the contribution of low trusted paths. Starting from the source node, the trust inference is calculated by averaging the trust (direct or inferred) for the sink node reported by all the directly connected trusted nodes (neighbors). More in detail, the aggregation of the trust coming from the different paths is obtained as a weighted average, where the reported trust is weighted by the reputation of the neighbors. The trust inference function is recursively computed along the paths in order to propagate the trust up to the target node.

A. Handling Controversial Cases with TrustZic

In this section we will give some preliminary numerical examples in order to show how *TrustZic* is able to address controversial cases by exploiting the reputation of the intermediate nodes. We consider a trust range $TR = [0,1]$, so that $T(i,j) \in [0,1]\ \forall(i,j) \in E$. $T(i,j) = 1$ means that user i fully trusts user j, while $T(i,j) = 0$ means lack of trust.

For the sake of simplicity and to isolate the reputation effect, only in this explanatory example, all the trust opinions will be considered equal to 1, while the lack of trust is uniformly considered equal to 0, and the effect of the trust decay with the path length is neglected ($d = 1$).

Figures 4, 5 and 6 show three different controversial cases. In the first case (Fig. 4), a node *Z* receives two opposite trust opinions from nodes *B* and *C*, propagated up to node *A*. In this case, the reputation of nodes *B* and *C* is the same due to the symmetric configuration, thus the resulting inferred trust is exactly the mean of the two reported trust opinions ($IT(A,Z) = 0.5$).

This is a critical situation when trust inference is used to take decisions. In fact, trust inference can be used as a decision support system by setting a trust threshold value for delimiting the trusting by the no-trusting zones. A generic node *X* decides to trust another node *Y* only if the inferred trust from the network is above a fixed threshold. In this specific example, if the threshold is reasonably set to the intermediate value ($Thres = 0.5$) of the $[0,1]$ trust range, no decisions can be taken because the inferred trust is exactly equal to the threshold (IT(*A*, *Z*) = 0.5 = $Thres$).

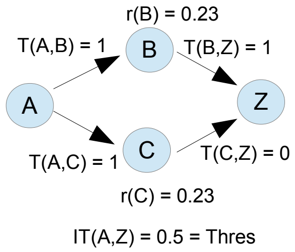

Fig. 4. An undecidable controversial case.

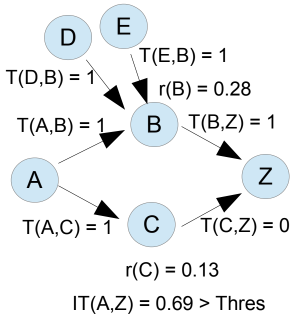

Fig. 5. The controversial case resolved by *TrustZic* due to the increased reputation of node *B*.

The second and the third cases (Figures 5 and 6) consider the connections of the rest of the trust network with nodes *B* and *C*, and their effects on their reputation. In the second case, the reputation of node *B* is higher (r(*B*) = 0.28) than that of *C* (r(*C*) = 0.13) because of the two nodes (*D* and *E*) trusting *B*. In the third case, the reputation of node *C* is further decreased (r(*C*) = 0.12) as a consequence of the 0-trust inner edge from (*F*). The effects of the reputation changes become relevant for the resolution of the controversial case in the inferred trust between nodes *A* and *Z*. In fact, in the cases reported in Figures 5 and 6, the inferred trust allows to easily take decisions: node *A* will trust node *Z* because the reputation of node *B*, reporting a positive opinion, is higher than that of node *C*, reporting a lack of trust opinion.

V. Experimental evaluation

A. Data

The proposed trust inference algorithm was evaluated through experiments conducted on Advogato, a real social network which is considered a de-facto benchmark for trust analysis tasks. Advogato.org is an online community platform for free software developers, which also served as a research

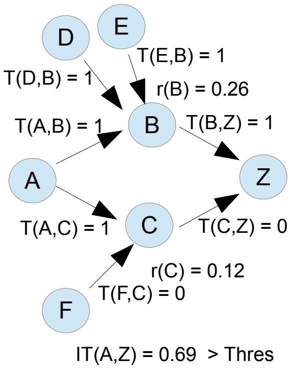

Fig. 6. The controversial case resolved by *TrustZic* due to the decreased reputation of node *C*.

testbed for testing an attack-resistant trust metric. Edges in the Advogato network graph are labeled according to three different levels of certifications (trust links), namely *master*, *journeyer*, *apprentice*; a user without any trust certificate is called an *observer*. The Advogato trust metric uses this information in order to assign to every user a certification level, in order to reduce the impact of attackers, e.g., apprentices can only post comments, whereas journeyers and masters are able to post both stories and comments. The Advogato network dataset was built by aggregating the daily-snapshot graph files available at the www.trustlet.org site, which cover the period Jan 1, 2008 - Apr 2, 2014 [20]. Each link from user u to user v, in the final aggregated graph, is labeled with the last certification given by u to v.

B. Methodology

Our experimental analysis was divided in two phases. The first phase is aimed at studying the error prediction performances of the proposed technique in terms of *MAE*. MAE (Mean Absolute Error) is a well-known metric used to represent the prediction error of a set of trust edges in a trust network. The prediction error is calculated as the displacement between a trust value in a trust network and the corresponding inferred trust value calculated after removing the edge from the network. The average of the prediction errors calculated for each trust edge in a dataset yields the MAE value. When the controversy level of the inferred trust values is used to group the edges of the entire dataset, an analysis of the MAE versus controversy distribution is used to study the performances of the proposed technique at different levels of controversy.

The second phase is aimed at evaluating the performances of the proposed technique in the trust decision problem. The *accuracy* and *F-score* measures are calculated with respect to the controversy levels. More in detail, a threshold $Thres$ is used to establish if a generic node X will trust another node Y based on the calculated inferred trust $IT(X,Y)$. Only if the inferred trust is higher than the threshold ($IT(X,Y) > Thres$), X will trust Y. For the computation of the accuracy and the F-score, TP (True Positive), TN (True Negative), FP (False Positive) andFN (False Negative) were measured with respect to the trust T and inferred IT values, as follows:

$$\begin{gathered} TP \text{ iff } T > Thres \text{ AND } IT > Thres \\ TN \text{ iff } T \leq Thres \text{ AND } IT \leq Thres \\ FP \text{ iff } T \leq Thres \text{ AND } IT > Thres \\ TN \text{ iff } T > Thres \text{ AND } IT \leq Thres \end{gathered}$$

The *accuracy* and *f-score* of the prediction are calculated as follows:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{11}$$

$$F - score = 2 \times \frac{TP}{2TP + FP + FN} \tag{12}$$

Experiments were carried out using three different algorithms: *TrustZic*, *TidalTrust* and *NeighborTrust*.

The *NeighborTrust* of a node is a baseline measure calculated by averaging the trust opinions from its in-neighbors. The use of the only direct trust values without any form of propagation and aggregation across the network is a common approach often used for its simplicity. In *TidalTrust* [14], previously mentioned in Section III-A, trust is propagated along the paths from the source node to the target. In order to take into consideration the fact that low trusted nodes are not affordable for trust propagation, a trust threshold ($Thres$) is introduced for filtering the low trusted paths from the computation. For any two nodes A, B, *TidalTrust* computes the following value of trust:

$$T(A,Z) = \frac{\sum_{\substack{K \in adj(A) \\ T(A,K) > Thres}} T(A,K) \times T(K,Z)}{\sum_{\substack{K \in adj(A) \\ T(A,K) > Thres}} T(A,K)} . \tag{13}$$

C. Results

In order to explore the behavior of the different algorithms in the presence of controversial conditions, MAE, accuracy and F-Score performances were tested as a function of controversy measured as in (6). Thus, the range of NTC values was divided in intervals of size 0.1, where each bin represents the percentage of trust edges falling in the specific NTC interval (so that all frequency values sum up to 100%).

Results are reported in Figures 8–7. Figure 7 shows the MAE vs. NTC histogram that reports the distribution of trust prediction error w.r.t. the level of NTC, i.e., the average error for the edges showing an NTC in each specified interval. In the accuracy vs. NTC histograms of Figures 8, 9, 10, and the F-Score vs. NTC histograms of Figures 11, 12, 13 we show the distribution of the average of accuracy and F-Score for the edges showing an NTC in each specified interval for different threshold values, $Thres = 0.4$, 0.5 and 0.6, respectively.

Considering first MAE vs. NTC histograms in Figure 7, we observe three different behaviors. For low levels of controversy ($0 \leq NTC \leq 0.2$), even if the MAE average values of the selected trust inference methods are very similar, the

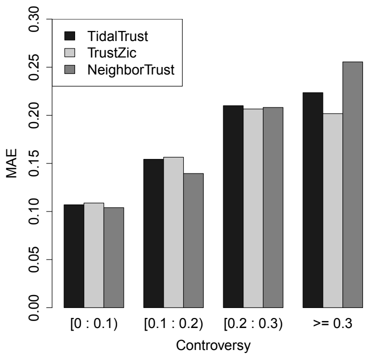

Fig. 7. The MAE vs. NTC distribution of trust edges.

NeighborTrust shows the lowest levels of error prediction. This behavior can be explained by the fact that when users agree in trusting opinions (low levels of controversy), there is no ambiguity, and the trust inference can be simply predicted as the average of the trust opinions by the in-neighbors. For intermediate levels of controversy ($0.2 \leq NTC \leq 0.3$) the three methods have nearly the same performances. When the controversy level increases ($NTC \geq 0.3$), the *NeighborTrust* shows the worse prediction. *TidalTrust* offers better results because personalization is preserved by the fact that only the paths form the source to the sink are taken in consideration, thus removing controversial trust opinions that are not related to the source node. The best prediction score in terms of MAE is reached by *TrustZic* because it uses the global reputation of the intermediate nodes to help in the disambiguation of the controversy, in fact, the nodes in the trust paths have different weight depending on the global reputation (credibility), assigned by the entire trust network.

A similar behavior is reported for the accuracy and F-score performances. Coherently with the assumptions made for the controversial explanatory examples, when the level of controversy increases ($NTC \geq 0.3$), the best accuracy and the F-score results are reached by the proposed approach. More in details, the phenomenon is more evident for higher values of threshold ($Thres = 0.6$) where, on average, the F-score values of *TidalTrust* and *NeighborTrust* are 28% and 92% lower than those reached by *TrustZic*, respectively.

A major aspect to be highlighted is the fact that when the controversy level grows, our *TrustZic* shows better results, coherently with the purpose of the proposed approach which has been conceived to give support in ambiguous more controversial situations.

VI. Conclusion

Trust regulates relations among people, in offline relations as well as in online social networks and web communities, where the interaction among users in the absence of any direct connection can easily happen. In this context, trust inference algorithms are a fundamental tool to estimate missing trust

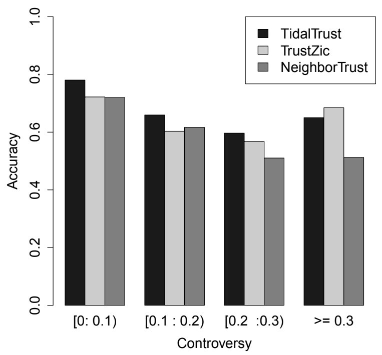

Fig. 8. The accuracy vs. NTC distribution of trust edges for $Thres = 0.4$.

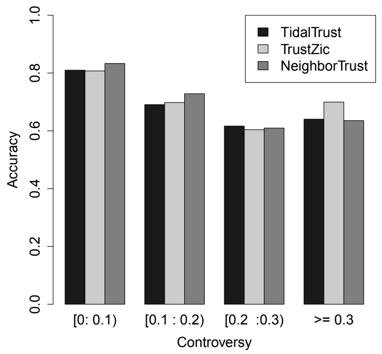

Fig. 9. The accuracy vs. NTC distribution of trust edges for $Thres = 0.5$.

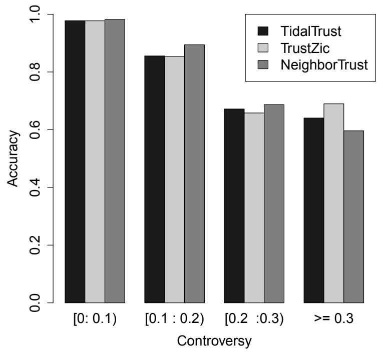

Fig. 10. The accuracy vs. NTC distribution of trust edges for $Thres = 0.6$.

evaluations. Controversial situations caused by disagreement in the existing trust statements towards a user need to be specifically taken into account during the inference process. In this work we proposed a novel trust inference algorithm, *TrustZic*, in which global and local trust aspects are combined, in order to infer reliable trust values also in presence of controversial situations. Experiments conducted on a real-world trust network has shown the significance and effectiveness of

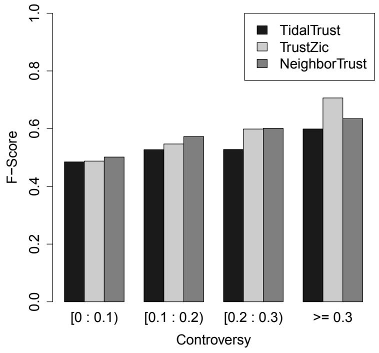

Fig. 11. The F-Score vs. NTC distribution of trust edges for $Thres = 0.4$.

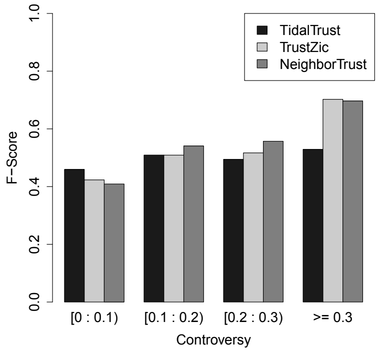

Fig. 12. The F-Score vs. NTC distribution of trust edges for $Thres = 0.5$.

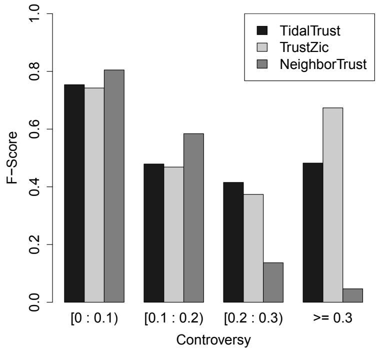

Fig. 13. The F-Score vs. NTC distribution of trust edges for $Thres = 0.6$.

our approach in solving critical trust inference scenarios.

Acknowledgements. This work was partly supported by the Cyber Security Technological District funded within the Italian National Operational Programme for Research and Competitiveness 2007-2013 under grant number PON03PE_00032_1.

References

[1] W. Jiang, G. Wang, M. Z. A. Bhuiyan, and J. Wu, "Understanding graph-based trust evaluation in online social networks: Methodologies and challenges," *ACM Comput. Surv.*, vol. 49, no. 1, pp. 10:1–10:35, 2016.

[2] W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," *ACM Comput. Surv.*, vol. 45, no. 4, pp. 47:1–47:33, 2013.

[3] Z. Gyöngyi, H. Garcia-Molina, and J. Pedersen, "Combating web spam with trustrank," in *Proc. of Conf. on Very Large Data Bases (VLDB)*, 2004, pp. 576–587.

[4] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The Eigentrust Algorithm for Reputation Management in P2P Networks," in *Proc. of Conf. on World Wide Web (WWW)*, 2003, pp. 640–651.

[5] R. Aringhieri, E. Damiani, S. D. C. Di Vimercati, S. Paraboschi, and P. Samarati, "Fuzzy techniques for trust and reputation management in anonymous peer-to-peer systems," *J. Am. Soc. Inf. Sci. Technol.*, vol. 57, no. 4, pp. 528–537, 2006.

[6] P. Massa and P. Avesani, "Trust metrics on controversial users: Balancing between tyranny of the majority," *Int. J. Semantic Web Inf. Syst.*, vol. 3, no. 1, pp. 39–64, 2007.

[7] ——, "Controversial users demand local trust metrics: An experimental study on epinions.com community," in *Proc. of National Conf. on Artificial Intelligence and Conf. on Innovative Applications of Artificial Intelligence*, 2005, pp. 121–126.

[8] P. Victor, C. Cornelis, M. D. Cock, and A. Teredesai, "A comparative analysis of trust-enhanced recommenders for controversial items," in *Proc. AAAI Conf. on Weblogs and Social Media (ICWSM)*, 2009.

[9] P. Zicari, R. Interdonato, D. Perna, A. Tagarelli, and S. Greco, *Controversy in Trust Networks*, ser. LNCS 9824. Springer International Publishing, 2016, pp. 82–100. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-45572-3˙5

[10] J. Golbeck, B. Parsia, and J. A. Hendler, "Trust networks on the semantic web," in *Workshop on Cooperative Information Agents (CIA)*, 2003, pp. 238–249.

[11] W. Jiang, G. Wang, and J. Wu, "Generating trusted graphs for trust evaluation in online social networks." pp. 48–58, 2014.

[12] S. Nepal, W. Sherchan, and C. Paris, "Strust: A trust model for social networks," in *Proc. of IEEE Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2011, pp. 841–846.

[13] S. Adali, R. Escriva, M. K. Goldberg, M. Hayvanovych, M. Magdon-Ismail, B. K. Szymanski, W. A. Wallace, and G. T. Williams, "Measuring behavioral trust in social networks," in *Proc. of IEEE Conf. on Intelligence and Security Informatics (ISI)*, 2010, pp. 150–152.

[14] J. A. Golbeck, "Computing and applying trust in web-based social networks," Ph.D. dissertation, College Park, MD, USA, 2005.

[15] L. Page, S. Brin, R. Motwani, and T. Winograd, "The pagerank citation ranking: Bringing order to the web," Stanford, USA, Tech. Rep., 1999.

[16] S. Hamdi, A. Bouzeghoub, A. L. Ganarski, and S. B. Yahia, "Trust inference computation for online social networks." in *Proc. of IEEE Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom) / IEEE Symposium on Parallel and Distributed Processing with Applications (ISPA) / IEEE Conf. on Ubiquitous Computing and Communications (IUCC)*, 2013, pp. 210–217.

[17] P. Victor, C. Cornelis, M. D. Cock, and A. Teredesai, "Trust- and distrust-based recommendations for controversial reviews," *IEEE Intelligent Systems*, vol. 26, no. 1, pp. 48–55, 2011.

[18] C. Haydar, A. Roussanaly, and A. Boyer, "Local trust versus global trust networks in subjective logic," in *Proc. IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT)*, 2013, pp. 29–36.

[19] M. Tang, Y. Xu, J. Liu, Z. Zheng, and X. F. Liu, "Combining global and local trust for service recommendation," in *Proc. of IEEE Conf. on Web Services (ICWS)*, 2014, pp. 305–312.

[20] R. Interdonato and A. Tagarelli, "To trust or not to trust lurkers?: Evaluation of lurking and trustworthiness in ranking problems," in *Proc. Int. School and Conf. on Network Science (NetSciX)*, ser. LNCS 9564, 2016, pp. 43–56.