On the impact of trust relationships on social network group formation

Lidia Fotia*, Fabrizio Messina†, Domenico Rosaci*, Giuseppe M. L. Sarné ‡
*DIIES, University of Reggio Calabria, Italy, {lidia.fotia,domenico.rosaci}@unirc.it
†DMI, University of Catania, Italy, messina@dmi.unict.it
‡DICEAM, University of Reggio Calabria, Italy, {sarne}@unirc.it

***Abstract*—Members of virtual communities generally expect that their groups satisfy some given requirements. For this aim, the profile matching between user requirements and group characteristics can be considered as the most natural way to represent the group homogeneity, measuring how much the group members are mutually linked. However, optimizing profile matching does not guarantee that the group will continue to be homogeneous in time (i.e., cohesive). In the past we have already shown that, when group formation is driven by trust measures and profile matching group homogeneity is improved. In this work, we prove by experiments on a dataset extracted from a real social network, that trust measures can be used to effectively replace profile matching for optimizing group's cohesion. Furthermore, we prove also that using a local trust measure will does not penalize the cohesion of the group.**

***Index Terms*—Cohesion, Homogeneity, Similarity, Trust, Virtual Communities.**

I. Introduction

Social networks, as Facebook [1] and Twitter [2], involve several users and online communities as, for example, those based on Internet Relay Chat. These communities are based on social relationship, as the *facebook friends* and the *twitter followers*: users form groups based on some thematic interests [3], but the groups are also created for representing classes in e-Learning activities, or set of customers interested in performing together e-Commerce purchases. Furthermore, some distributed systems as, Grid virtual organizations [4] or cloud of clouds [5], can be viewed as virtual communities whose members are software agents performing activities implying social interactions.

Two main activities are performed in a virtual community with reference to group formation: a potential group member looks for interesting groups and a group administrator manages a group. Consequently, a potential new member asks for joining with a group of interest and a group can accept or refuse the request of a potential new member. In this way, it is possible to produce groups whose members are satisfied of their memberships. In many cases, new members must meet some *requirements* to be part of a group. For this reason, in [6], we have extended the concept of profile similarity to define a measure, called *Average Similarity*, that represents the global, mutual satisfaction perceived by the members of a group of a virtual community. This measure takes into account the similarity between the profiles of two members (i.e., interests and preferences). Therefore, for a given group, we define the average satisfaction computed on entire

In this work, we introduce a new measure, called *Average Matching*. The *profile matching* between user's requirements and group's characteristics can be considered to represent the *group homogeneity*, measuring how much the group members are mutually linked. But, it is not said that the group will continue to be homogeneous in time (i.e., *cohesive*). Furthermore, an agent, when declaring some characteristics of the profile, could be fraudulent, and this can affect the effectiveness of the matching. For this reason, in [6], we introduce the *trustworthiness* between two members. Moreover, computing profiles similarities is not always possible because the user do not make publicly available such information in order to preserve his/her privacy [7]–[11]. In our past approach, we define another measure, called *Average Compactness*, taking into account both the similarity and the trustworthiness. On the basis of this measure, we have introduced an algorithm, called User-to-Group (U2G), able to heuristically provide a good solution to the problem of maximizing the Mean Average Compactness (MAS) of all the groups of the social community. Clearly, groups formed based on compactness, should be capable to exhibit an internal cohesion in time, even in absence of information about profile matching. In this paper, we define a criterion for measuring the actual capability of the group to not decreasing in time the mutual profile matching of their members. Secondly, in [6], we have used a measure of the trustworthiness, only by taking into account the direct knowledge. However, in many cases, it is impossible to estimate the trustworthiness because the agents have not had direct contacts. To solve this problem, we have considered the possibility to use both the direct experience of interaction occurred with a (*target*) agent (i.e., *reliability*), and the past experiences of the whole set of the agents present in the community with the same target agent (i.e., *reputation*). Moreover, in [12], we integrate the traditional use of the global reputation with the *local reputation*, that is based on recommendations only coming by the entourage of the user. The experiments showed that the use of local reputation improves the effectiveness of the recommendations with respect to the use of the global reputation and, in most of the cases, the use of the sole local recommendation is the best choice. In this paper, as a second contribution, we propose to compare the use of the local reputation vs the simple reliability when using the algorithm U2G for automatically forming groups in virtual communities.

II. Related Work

A relevant research area investigate on virtual communities [13]–[16] often composed by humans and software agents. In this context, trust affects decisional processes and social interactions [17]–[21] so that several approaches deal with the problem of *group recommendation* and *group affiliation* to take benefits or mitigate risks for unreliable partners [22]–[24]. To identify the best items to suggest to a group, some approaches adopt a *score aggregation* strategy to build a group profile. In this scenario, two popular strategies are the *Average* [25] and the *Least Misery* [26]. Conversely, other approaches match users and group information [27]. In [28], the authors propose a probabilistic approach to recommend new friends to users, where a *bag of users* and a *bag of words*, describing a community and its interests, are built and combined to improve their data sparsity degree. Differently, in Vasuki *et al.* [29] study the co-evolution of the user's friendship relationships and the knowledge of group affiliations are used to predict the next groups to join with.

Other studies model trust in social communities by means of a graph (usually sparse), defined *trust network*, whose vertexes represent the users and oriented edges represent trust relationships. For example, in [30] a maximum network flow algorithm infers trust and in [31] a modified Breadth First Search collects multiple reputation scores, basing on a voting algorithm, and returns a unique reputation rate for each user. The trust can be calculated in different ways [32]–[37]. The first one consists of direct opinions based on personal past experiences and indirect information provided by other users. In the other way, trust can be computed by adopting a local or a global approach in a centralized or distributed way. Some researches states as the local trust is the more accurate when personal users' point of views are adopted [38] with a computational cost depending on the horizon chosen to discovery a *trust* chain linking two users [39]. Finally, there exist some approaches that have been tested on real dataset, as in our proposal [40], [41]. In particular, SoReg [41] provides a method to improve recommendations to include social network context, by using a matrix factorization framework with social regularization.

III. The proposed ego-network model

Our scenario is represented by a virtual community $\mathcal{C}$, denoted as $\mathcal{C} = \langle \mathcal{A}, \mathcal{G}, \mathbf{m}, \mathbf{t} \rangle$, where $\mathcal{A}$ is the set of *agents* and $\mathcal{G}$ is the set of *groups*, while $\mathbf{m}$ and $\mathbf{t}$ are two mappings denoting the *matching* and the *trust* metric.

Each group g is managed by an administrator agent a_g. Furthermore, each agent and each group owns a profile p_x defined as a list of n property values, i.e. $p_x = \{\rho_x^1, \rho_x^2, .., \rho_x^n\}$. Each property ρ_x^i, $i = 1, 2, .., n$ represents the value assumed by a specific aspect characterizing the agent x in the community.

The matching metric is a mapping that receives as input two agents and yields as output a real value, ranging in the interval $[0 \cdots 1]$. The profile matching metric is *symmetric* and explains how much the values of the profile properties of an agent match with the values of the corresponding properties of another agent. It is computed as follows: $\mathbf{m}(x, y) = \dfrac{\sum_{i=1}^{n}(\rho_x^i - \rho_y^i)}{n}$, where we assume that an appropriate operator "$-$"is defined for each property ρ^i, that returns a real value in the interval $[0 \cdots 1]$. Clearly, 0 means that there is not a matching between x and y. The matching between an agent and a group is defined in the following way: $\mathbf{m}(x, g) = \dfrac{\sum_{y \in g} \mathbf{m}(x, y)}{|g|}$, where $|g|$ denotes the cardinality of group g.

The *trust* $\mathbf{t}(x, y)$ is a mapping that receives as input two agents and yields as output a boolean value representing the degree of trust. The trust metric is *asymmetric*. In the same way, the trust perceived by an agent with respect to a group is defined as:

$$\mathbf{t}(x, g) = \frac{\sum_{\{y \in g : \mathbf{t}(x,y) \neq NULL\}} \mathbf{t}(x, y)}{|\{x \in g : \mathbf{t}(x, y) \neq NULL\}|}$$

where $\mathbf{t}(x, y) \neq NULL$ when a couples of agents had some interactions in the past. We assume that $\mathbf{t}(x, y)$ is composed by two components: *reliability* and *reputation*. The reliability, denoted by $\mathbf{rel}(x, y)$, that x assigns to y in consequence of the direct experience made in past interactions assumes values ranging in the domain $[0 \cdots 1] \cup \{NULL\}$. The reputation, denoted by rep_y, represents the reputation that y has in the community in the interval $[0 \cdots 1] \in \mathbb{R}$. To compute the reputation, we adopt the notion of *local reputation* [12]. Let $G = \langle N, A \rangle$ be a directed unlabeled graph associated with the virtual community $\mathcal{C}$, where N is a set of nodes and A is a set of arcs. Each node is associated with an agent, while each arc is a pair (h, l), with $h, l \in N$ representing a reliability link existing in $\mathcal{C}$ between the agents a_h and a_l. Moreover, let $n(x)$ be the node of the graph corresponding to the agent x.

The *ego-network* of an agent x will be defined as the subgraph of G, denoted by G_x, that represents all the agents both directly and indirectly trusted by x. Hereafter, we say that an agent y belongs to the ego-network of x if the node $n(y)$ belongs to G_x. We assume that $local_{trust}$ is a relation defined on $A \times A$, such that an ordered pair of agents belongs to $local_{trust}$ only when the node $n(y)$ belongs to the ego-network G_x of x. Also, for all the nodes $n(x)$, $n(y)$ such that $[x, y] \in local_{trust}$ we also define a (normalized) local reputation measure $l_{rep}(x, y)$ which represents how much the agents belonging to the ego-network G_x of x trusts y. We compute local reputation by suitably summing the contributions (in terms of trust in y) coming by all the users k (with $k \neq x$) belonging to the ego-network of x which results to be also connected with y.

Let $total(x, y)$ be this sum, and we call *local network*, denoted by $l_{net}(a, b)$, the set of contributors, $l_{net}(x, y) = \{z : z \in G_x \wedge \exists(z, y) \in G_y\}$. If $k \in l_{net}(x, y)$ is a user in which x

directly trusts, then there exists an arc $(n(x), n(k)) \in G_x$. Our model assumes that the contribution of k to $total(x, y)$ is equal to 1. Otherwise, if k is indirectly trusted by x, then there exists at least one path in G_x which connects x and k. We assume that the shortest path between $n(x)$ and $n(k)$ belongs to G_x and suppose it has a length $l_{x,k}$. In this case, the contribution provided by k to the trust computation we propose be equal to $1/2^{l_{x,k}-1}$. Therefore, the formula adopted for the (normalized) local reputation is the following:

$$\mathbf{rep}(x, y) = \frac{\displaystyle\sum_{k\in l_{net}(x,y), k\neq x,y} \frac{1}{2^{l_{x,k}-1}}}{\displaystyle\max_{z\in A, z\neq x,y}\left(\sum_{h\in l_{net}(x,z), h\neq x,z} \frac{1}{2^{l_{x,h}-1}}\right)} \quad (1)$$

The two trust components are integrated in a unique value in the interval $[0, 1]$ as follows:

$$\mathbf{t}(x, y) = \beta_u \cdot \mathbf{rel}(x, y) + (1 - \beta_u) \cdot \mathbf{rep}(x, y) \quad (2)$$

where β_u is a real coefficient belonging to $[0..1]$ which is set by x to weight the relevance he/she assigns to the reliability with respect to the reputation.

IV. Cohesion and Compactness

Now, we introduce a measure to define how much a configuration of groups in $\mathcal{C}$ can be considered as *cohesive*. We denote the *Average Matching* as $M_g = \frac{\sum_{x,y\in g, x\neq y} \mathbf{m(x,y)}}{|g|}$, that measures how much the agents are mutually satisfied to stay in g. Then, we denote as *Mean Average Matching* (MAM), a measure of the internal mutual satisfaction of the whole configuration of groups S, defined as follows:

$$MAM = \frac{\sum_{g\in S} M_g}{h} \quad (3)$$

The goal is to improve the value of MAM until the maximum possible value. This problem is not an optimization problem, since the property values change in time, and the best we could do is to compute the optimum configuration at a given time t. Therefore, it is easy to see that finding this optimum is a NP-problem and it is not guarantee that this optimum at time t will be the optimum of MAM also at $t + 1$.

In this perspective, let S_0 be a configuration at a time t_0, then the higher the optimum of MAM at the time $t_0 + \Delta$, the better the *cohesion* of the configuration S_Δ at time $t_0 + \Delta$. Then, we define a measure called Δ-*Cohesion* $\Phi_\Delta(S)$, defined as follows: let S be a configuration of groups in a virtual community, considered at the time t_0 and let Δ be the time-window $[t_0, t + \Delta]$. We define Δ-*Cohesion* $\Phi_\Delta(S)$ as the MAM obtained at the end of the time-window $[t_0, t + \Delta]$. Therefore, a group configuration $S2$ having a $\Phi_\Delta(S2)$ greater than the $\Phi_\Delta(S1)$ of another group configuration $S1$, can be considered more cohesive than $S1$ in the given time-window Δ, since it finally produces groups that in average present better group matching values. We would define a rational strategy for leading the agents of the community to change in time the configuration of groups in order to maximize the Δ-cohesion.

Suppose that an agent $x \in g_1$ evaluates the possibility to change group by joining with g_2 because $\mathbf{m}(x, g_2) > \mathbf{m}(x, g_1)$. But, it is possible that this change lowers the cohesion of g_2. In this case, x could be led to make bad choices by some unreliable of even fraudulent agents. For this reason, in [6], we introduce the *convenience* of x to be in the same group with y by taking into account both matching and trust. We denoted it as $\mathbf{c}(x, y) = \omega \cdot \mathbf{m}(x, y) + (1 - \omega) \cdot \mathbf{t}(x, y)$, where ω is a real number, ranging in $[0 \cdots 1]$. Then, the *Average Convenience* is $C_g = \frac{\sum_{x,y\in g, x\neq y} \mathbf{c(x,y)}}{|g|}$. Finally, we can introduce the *Mean Average Convenience* (MAC) as follows:

$$MAC = \frac{\sum_{g\in S} AC_g}{h} \quad (4)$$

We define the measure called Δ-*Compactness* $\Upsilon_\Delta(S)$, defined as follows: let S be a configuration of groups in a virtual community, considered at the time t_0 and let Δ be the time-window $[t_0, t_0 + \Delta]$. We define Δ-*Compactness* $\Upsilon_\Delta(S)$ as the MAC obtained at the end of the time-window.

We can construct our groups having available a *training phase* $\Delta 1$, but at the end of this phase we would desire to have a group configuration that will result the best cohesive at the end of a *test phase* $\Delta 2 - \Delta 1$. In this case, we have uncertainty about the evolution of the agents' behaviors in the unknown time-window $\Delta 2 - \Delta 1$, and we could be deceiving when forming our groups in the training phase by the behavior of unreliable agents. A solution could be to form the groups in the training phase by using the compactness to take into account information about the agents' trustworthiness. Therefore, the configuration S_1^*, corresponding to the compactness $\Upsilon_{\Delta 1}(S_0)$ after the training phase, could produce a better cohesion $\Phi_{\Delta 2 - \Delta 1}(S_1^*)$ at the end of the test phase than the cohesion $\Phi_{\Delta 2 - \Delta 1}(S_1)$, produced by the configuration $S1$.

V. User-To-Group (*U2G*)

In this section, we sketch the design of the algorithm User-To-Group (*U2G*), which enables user agents to select the groups to join with by maximizing the values of compactness Υ (see Figure 1) .

We suppose that $\mathcal{G}$ is the set of n groups in $\mathcal{C}$. Moreover, let $k_{\texttt{MAX}}$ be a threshold ranging in $[0, n]$ which specifies the upper bound on the number of groups each user u desires to join with. Algorithm U2G has been designed to select $k_{\texttt{MAX}}$ groups yielding the largest value of the MAC computed on $\mathcal{G}$. We assume that as u joins with more than one group then each of them still continues to give the whole benefit to u, so that the overall benefit, in terms of MAC, received by u is equal to the sum of each contribution.

Therefore, in presence of an arbitrary number of groups $\mathcal{J} \subseteq \mathcal{G}$, the benefit gained by u in joining with all the groups

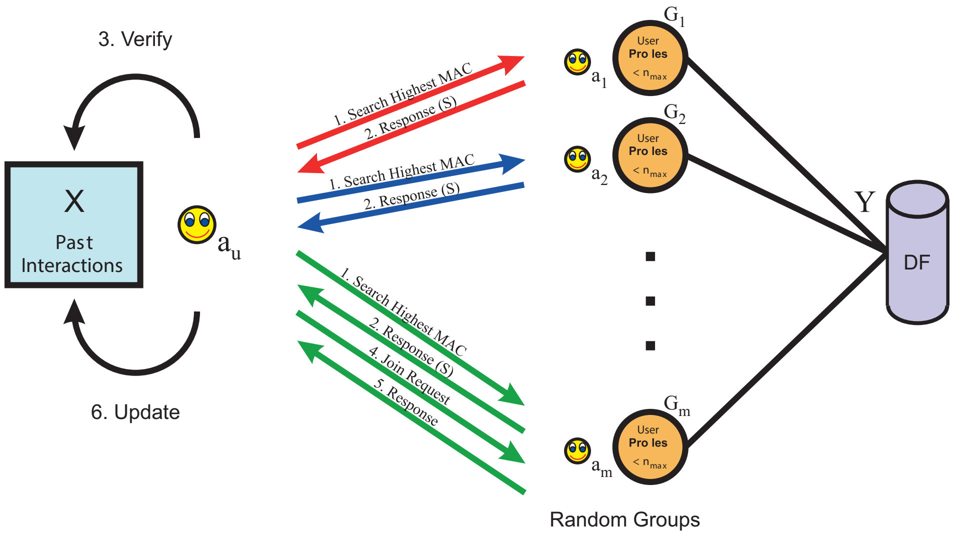

Fig. 1. User-To-Group.

in $\mathcal{J}$ is given by $\sum_{g_i \in \mathcal{J}} \gamma_{u \to g_i}$. The question of finding the subset $\mathcal{J}^\star \subseteq \mathcal{G}$ producing the best benefit for u under the constraint $|\mathcal{J}^\star| = k^u_{\mathtt{MAX}}$ is equivalent to solve an optimization problem.

As shown in Figure 1, the user a_u is able to sample m random groups from $\mathcal{G}$, where m is the number of the group agents that at each epoch must be contacted by a_u. Furthermore, a_u will record into an internal cache the profiles of the groups with which joined in the past; we shall denote this set as X. a_u performs various steps to find the $k_{\mathtt{MAX}}$ groups to which u can join.

It is assumed that the size of each group cannot be bigger than a threshold $n_{\mathtt{MAX}}$, (a value fixed by the group administrator) and each agent a_g stores into an internal cache the profiles of the users who joined g. In particular, let Y be a set of m random groups extracted from DF and $Z = X \bigcup Y$.

For each group g in Y, a_u sends a message to the agent a_g. Let s be the set of $k_{\mathtt{MAX}}$ group of Z having the highest values of MAC. For each g in S, if $g \notin X$, a_u sends a join request to the agent a_g that also contains the profile p_u of u. Otherwise, a_u deletes u from g. In this way, we obtain the set Z. In our example, a_u sends the join request only to the group g_m, that has the highest value of MAC. Finally, a_u updates the set X. In [6], we show the corresponding algorithm implemented by the group agent.

VI. Experiments

In this section we discuss the results obtained by the executing the algorithm U2G on a real datasets, extracted from the social networks CIAO, described in [40]. CIAO dataset consists in a matrix with a total of about 36k rows, each of them represents an event in the virtual community, in the form {*userID, productID, categoryID, rating*, helpfulness, *timestamp*}. In particular, *rating* is a value assigned to the product by the user and the helpfulness represents the level of satisfaction of the other users for that rating. In addition, a dataset representing trust relationships is available. It consists in a list of pairs of user, where each of them represents a trust relationship among two users.

In our experiments, we have associated with each user a profile containing the expertise of the user in reviewing products, computed by averaging the helpfulness associated with each review posted by the user. Conversely, the reliability is represented by the values found in the dataset of trust relationships, while reputation has been calculated based on Eq. 1 (Section III). We make the following assumptions, necessary for the simulation campaign. The rows of the dataset are arranged in an increasing order based on the timestamp and the dataset is divided into 11 time-windows Δ. The first time-window is used as training set, the remaining ten are used for the subsequent tests. Then, the reliability matrix is constructed by loading the dataset containing trust relationships and the training is performed by executing the algorithm *U2G* on the first time-window Δ_1. At the end of this phase, a cohesion Φ_{Δ_1} is measured. The test phase is performed by computing subsequent cohesion values, by adding data of time-windows $\Delta_2, \ldots, \Delta_{end}$, until the final value $\Phi_{\Delta_{end}}$ is found.

The goal is to understand the ability to form cohesive groups on the basis of the trust measure. In particular, we are interested in comparing final values of cohesion, i.e. $\Phi_{\Delta_{end}}$, among the different categories used to perform the training test (i.e., training based on matching, training based on matching and trust, and training based on trust only). For this reason, we performed a number of experiments that can be divided into these categories (see Table I). Also, ω is the weight assigned to the matching in the computation of the compactness, therefore $\omega = 1$ means that only matching is considered, while $\omega = 0$ means that only the trust contribution is actually weighted in the computation of compactness; β is the weight which balance trust and reputation. The column

Training	ω	β	**Local Reputation**	CIAO	
				Ψ_{Δ_1}	$\Psi_{\Delta_{end}}$
only matching	1	–	–	0.69	0.74
matching and reliability	0.5	1	0	0.68	0.74
matching and reliability+reputation	0.5	0.5	1	0.69	0.73
matching and reputation	0.5	0	1	0.70	0.74
reliability	0	1	0	0.71	0.78
reliability+reputation	0	0.5	1	0.60	0.80
reputation	0	0	1	0.69	0.78

TABLE I
SUMMARY OF THE EXPERIMENTAL RESULTS

$LocalReputation$ is a flag used to distinguish two different cases. If $LocalReputation$ is set to 1, we consider a trust using both local reputation and reliability, weighted by β. Otherwise, we use only the local reputation.

In the case of CIAO, reliability is a boolean value and it does not allow us to make the distinction mentioned above. For this reason, we used a variation of Eq. 2 that formula, as follows:

$$\mathbf{t}(x,y) = \begin{cases} \beta\ rel(x,y) + (1-\beta)\ rep(x,v) & \mathbf{rel}(1,y) \neq 0 \\ rep(x,y) & \mathbf{rel}(1,y) = 0 \end{cases} \tag{5}$$

A. Evaluation

In this first set of experiments, we have compared the final cohesion of groups when the training is performed by considering only the matching criteria, and that obtained by mixing matching and trust (i.e., matching and reliability, matching and reliability with reputation and matching and reputation).

The first result is represented by the fact that forming groups by considering also the reliability does not degrade the cohesion of the groups since $\Phi_{\Delta_{end}}$ is not subject to significant variation on its presence. If the training is still performed on the base of matching and trust, and the trust component is represented by a mix of reliability and local reputation, the contribution given by the reputation does not lead negative changes of $\Phi_{\Delta_{end}}$. Finally, in the case on which groups are formed by means of a training based on the mix between matching and local reputation, we observe that using the local reputation does not lead negative changes of $\Phi_{\Delta_{end}}$. By this, it is clear that local reputation can be used in place of reliability when groups are formed by mixing matching and trust.

Now, we compare the value of $\Phi_{\Delta_{end}}$ obtained for matching only, with that obtained for reliability, reliability with reputation and reputation. By setting parameter $\omega = 0$, only trust is included in the computation of compactness, used in the training phase, in order to form groups. Observe that $\Phi_{\Delta_{end}}$ are larger than values obtained in the previous cases for CIAO. In particular, if we use only the reliability value (i.e., $LocalReputation = 0$ and $\beta = 1$), we do not observe degradation in the cohesion of groups. Instead, even a little improvement of about 5% is obtained for CIAO, if compared with the previous case.

In conclusion, in the case of reputation only, we can say that local reputation, i.e. suggestions given by friends and friends of friends, can be effective in forming cohesive groups as much as direct knowledge, as it gives almost identical value of cohesion. Another important result is represented by the case reliability + reputation, in which we have an increase of $\Phi_{\Delta_{end}}$ of about 8%.

VII. CONCLUSION

In this work, we have defined a theoretical agent framework and applied it to the dataset extracted from the CIAO social network. In particular, we propose to represent the attitude of a group to maintain its internal homogeneity in a time interval Δ by a measure called Δ-cohesion, based on the profile matching. Then, we have defined another measure, mixing profile matching and trust, denoted as compactness. Finally, we have tried to form groups on the real social networks of reference by optimizing, at time t_0 the compactness, and by comparing our results with those obtained forming groups only based on the profile matching optimization. In both cases, the results are represented in terms of Δ-cohesion. Moreover, we have considered two different types of trust measures, namely the reliability and the local reputation. From the experiments, we can conclude that trust, and in particular local reputation, is a powerful tool to substitute profile matching for forming cohesive groups.

In the next future, we will try to go deeper into this result by performing a simulation campaign on a dataset extracted from an extensive social network.

REFERENCES

[1] Facebook, "https://www.facebook.com/," 2014.

[2] Twitter, "https://www.twitter/," 2014.

[3] F. Buccafurri, L. Fotia, and G. Lax, "Allowing continuous evaluation of citizen opinions through social networks," in *International Conference on Electronic Government and the Information Systems Perspective*. Springer, 2012, pp. 242–253.

[4] I. Foster, C. Kesselman, and S. Tuecke, "The anatomy of the grid: Enabling scalable virtual organizations," *International journal of high performance computing applications*, vol. 15, no. 3, pp. 200–222, 2001.

[5] N. Grozev and R. Buyya, "Inter-cloud architectures and application brokering: taxonomy and survey," *Software: Practice and Experience*, vol. 44, no. 3, pp. 369–390, 2014.

[6] P. De Meo, E. Ferrara, D. Rosaci, and G. M. L. Sarnè, "Trust and compactness in social network groups," *ACM Transactions on Cybernetics*, vol. 45, no. 2, pp. 205–2016, 2015.

[7] F. Buccafurri, L. Fotia, and G. Lax, "Privacy-preserving resource evaluation in social networks," in *Privacy, Security and Trust (PST), 2012 Tenth Annual International Conference on*. IEEE, 2012, pp. 51–58.

[8] ——, “Allowing privacy-preserving analysis of social network likes,” in *Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on*. IEEE, 2013, pp. 36–43.

[9] ——, “Allowing non-identifying information disclosure in citizen opinion evaluation,” in *Technology-Enabled Innovation for Democracy, Government and Governance*. Springer, 2013, pp. 241–254.

[10] ——, “Social signature: Signing by tweeting,” in *International Conference on Electronic Government and the Information Systems Perspective*. Springer, 2014, pp. 1–14.

[11] F. Buccafurri, L. Fotia, G. Lax, and V. Saraswat, “Analysis-preserving protection of user privacy against information leakage of social-network likes,” *Information Sciences*, vol. 328, pp. 340–358, 2016.

[12] P. De Meo, F. Messina, D. Rosaci, and G. M. L. Sarné, “Recommending users in social networks by integrating local and global reputation,” in *Proceedings of the 7th International Conference on Internet and Distributed Information Systems. Lecture Notes in Computer Science Volume 8729*. Springer, 2014, pp. 437–446.

[13] A. Comi, L. Fotia, F. Messina, G. Pappalardo, D. Rosaci, and G. M. L. Sarné, “Forming homogeneous classes for e-learning in a social network scenario,” in *Intelligent Distributed Computing IX*. Springer, 2016, pp. 131–141.

[14] A. D. Rathnayaka, V. M. Potdar, T. S. Dillon, and S. Kuruppu, “Formation of virtual community groups to manage prosumers in smart grids,” *International Journal of Grid and Utility Computing*, vol. 6, no. 1, pp. 47–56, 2014.

[15] M. Pandey, V. K. Pathak, and B. D. Chaudhary, “A framework for interest-based community evolution and sharing of latent knowledge,” *International Journal of Grid and Utility Computing*, vol. 3, no. 2-3, pp. 200–213, 2012.

[16] Y. Huang, N. Bessis, P. Kuonen, and B. Hirsbrunner, “Casp: a community-aware scheduling protocol,” *International Journal of Grid and Utility Computing*, vol. 2, no. 1, pp. 11–24, 2011.

[17] D. Rosaci and G. Sarné, “Matching users with groups in social networks,” in *Intelligent Distributed Computing VII*. Springer, 2014, pp. 45–54.

[18] J. Heidemann, M. Klier, and F. Probst, “Online social networks: A survey of a global phenomenon,” *Computer Networks*, vol. 56, no. 18, pp. 3866–3878, 2012.

[19] A. Comi, L. Fotia, F. Messina, G. Pappalardo, D. Rosaci, and G. M. L. Sarné, “An evolutionary approach for cloud learning agents in multi-cloud distributed contexts,” in *2015 IEEE 24th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises*. IEEE, 2015, pp. 99–104.

[20] J. Zhan and X. Fang, “Social computing: the state of the art,” *International Journal of Social Computing and Cyber-Physical Systems*, vol. 1, no. 1, pp. 1–12, 2011.

[21] A. Comi, L. Fotia, F. Messina, G. Pappalardo, D. Rosaci, and G. M. L. Sarné, “Using semantic negotiation for ontology enrichment in e-learning multi-agent systems,” in *Complex, Intelligent, and Software Intensive Systems (CISIS), 2015 Ninth International Conference on*. IEEE, 2015, pp. 474–479.

[22] J. Fogel and E. Nehmad, “Internet social network communities: Risk taking, trust, and privacy concerns,” *Computers in Human Behavior*, vol. 25, no. 1, pp. 153–160, 2009.

[23] G. Lax and G. M. L. Sarné, “Celltrust: a reputation model for c2c commerce,” *Electronic Commerce Research*, vol. 8, no. 4, pp. 193–216, 2008.

[24] A. Comi, L. Fotia, F. Messina, D. Rosaci, and G. M. L. Sarné, “Grouptrust: Finding trust-based group structures in social communities,” in *International Symposium on Intelligent and Distributed Computing*. Springer, 2016, pp. 143–152.

[25] S. Amer-Yahia, S. Roy, A. Chawlat, G. Das, and C. Yu, “Group recommendation: Semantics and efficiency,” *Proc. of the VLDB Endowment*, vol. 2, no. 1, pp. 754–765, 2009.

[26] L. Baltrunas, T. Makcinskas, and F. Ricci, “Group recommendations with rank aggregation and collaborative filtering,” in *Proc. of the ACM Conf. on Recommender Systems 2010*. ACM Press, 2010, pp. 119–126.

[27] X. Liu, A. Datta, K. Rzadca, and E.-P. Lim, “Stereotrust: a group based personalized trust model,” in *Proc. of the 18th ACM conf. on Information and knowledge management*. ACM, 2009, pp. 7–16.

[28] W. Chen, D. Zhang, and E. Chang, “Combinational collaborative filtering for personalized community rrecommendation,” in *Proc. of the ACM Int. Conf. on Knowledge Discovery and Data mining (SIGKDD’08)*. ACM, 2008, pp. 115–123.

[29] V. Vasuki, N. Natarajan, Z. Lu, B. Savas, and I. Dhillon, “Scalable affiliation recommendation using auxiliary networks,” *ACM Transactions on Intelligent Systems and Technology*, vol. 3, no. 1, pp. 3:1–3:20, 2011.

[30] A.A.V.V., “Advogato’s trust metric,” 2013, `http://www.advogato.org/trust-metric.html`.

[31] J. Golbeck and J. Hendler, “Inferring binary trust relationships in web-based social networks,” *ACM Transactions on Internet Technology*, vol. 6, no. 4, pp. 497–529, 2006.

[32] D. Rosaci, G. M. L. Sarnè, and S. Garruzzo, “Integrating trust measures in multiagent systems,” *International Journal of Intelligent Systems*, vol. 27, no. 1, pp. 1–15, 2012.

[33] I. Pinyol and J. Sabater-Mir, “Computational trust and reputation models for open multi-agent systems: a review,” *Artificial Intelligence Review*, vol. 40, no. 1, pp. 1–25, 2013.

[34] D. Rosaci, G.M.L. Sarnè and S. Garruzzo, “TRR: An integrated reliability-reputation model for agent societies,” in *WOA 2011, Proc. of the 12th*, ser. CEUR Workshop Proc., vol. 741. CEUR-WS.org, 2011.

[35] A. Comi, L. Fotia, F. Messina, D. Rosaci, and G. M. Sarné, “A partnership-based approach to improve qos on federated computing infrastructures,” *Information Sciences*, vol. 367, pp. 246–258, 2016.

[36] M. N. Postorino and G. M. L. Sarné, “An agent-based sensor grid to monitor urban traffic,” in *Proceedings of the 15th Workshop from “Objects to Agents”, WOA 2014*, ser. CEUR Workshop Proceedings, vol. 1260. CEUR-WS.org, 2014.

[37] A. Comi, L. Fotia, F. Messina, G. Pappalardo, D. Rosaci, and G. M. Sarné, “A reputation-based approach to improve qos in cloud service composition,” in *Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2015 IEEE 24th International Conference on*. IEEE, 2015, pp. 108–113.

[38] P. Massa and P. Avesani, “Trust metrics on controversial users: Balancing between tyranny of the majority,” *International Journal on Semantic Web and Information Systems (IJSWIS)*, vol. 3, no. 1, pp. 39–64, 2007.

[39] C. Ziegler and G. Lausen, “Spreading activation models for trust propagation,” in *e-Technology, e-Commerce and e-Service, 2004. EEE’04. 2004 IEEE International Conference on*. IEEE, 2004, pp. 83–97.

[40] J. Tang, X. Hu, H. Gao, and H. Liu, “Exploiting local and global social context for recommendation,” in *Proceedings of the Twenty-Third International Joint Conference on Artificial Intelligence*, ser. IJCAI ’13. AAAI Press, 2013, pp. 2712–2718. [Online]. Available: http://dl.acm.org/citation.cfm?id=2540128.2540519

[41] H. Ma, D. Zhou, C. Liu, M. Lyu, and I. King, “Recommender systems with social regularization,” in *Proceedings of the fourth ACM international conference on Web search and data mining*. ACM, 2011, pp. 287–296.