



Trust-aware Recommendations

Christophe Courtin, Miguel Tomasena

► To cite this version:

Christophe Courtin, Miguel Tomasena. Trust-aware Recommendations. ISEEIE 2021: International Symposium on Electrical, Electronics and Information Engineering (published) / DMKD 2020: Data Mining and Knowledge Discovery (presented), Feb 2021, New York, NY, United States. pp.639-644, 10.1145/3459104.3459207 . hal-03295394

HAL Id: hal-03295394

<https://hal.science/hal-03295394v1>

Submitted on 4 Aug 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Trust-aware Recommendations

Christophe Courtin, Miguel Tomasena

► To cite this version:

Christophe Courtin, Miguel Tomasena. Trust-aware Recommendations. ISEEIE 2021: International Symposium on Electrical, Electronics and Information Engineering (published) / DMKD 2020: Data Mining and Knowledge Discovery (presented), Feb 2021, New York, NY, United States. pp.639-644, 10.1145/3459104.3459207 . hal-03295394

HAL Id: hal-03295394

<https://hal.archives-ouvertes.fr/hal-03295394>

Submitted on 4 Aug 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Trust-aware Recommendations

Christophe Courtin

SYMME, Université Savoie Mont Blanc, 73 376 Le
Bourget du Lac, France
courtin@univ-smb.fr

Miguel Tomasena

SYMME, Université Savoie Mont Blanc, 73 376 Le
Bourget du Lac, France
tomasena@gmail.com

ABSTRACT

When forming a work team, the choice of its members is a key step. We believe that a recommender system could help to select the members of a team by taking into account individual competences criteria, as well as the relationships between people. One important aspect of this relationship is the trust that members have with each other. However, this concept of trust remains difficult to be used because it is subject to many definitions and is complex to grasp. We try in this research to shed some light on the notion of trust. In particular, we study if there is a correspondence between a previously declared trust (off-line) and an actual trust put into practice during an experiment. To use the trust to recommend profiles of competences that stem from a wider and more reliable social network, we also investigate if the use of transitivity and reciprocity for trust makes sense.

CCS Concepts

Human-centered computing → **empirical studies in collaborative and social computing**

Keywords

Trust, Recommender System, Competence, Hard Skill, Soft Skill, Digital Trace of Interaction

ACM Reference format:

Christophe Courtin and Miguel Tomasena. 2021. Trust-aware Recommendations. In *Proceedings of 2021 International Symposium on Electrical, Electronics and Information Engineering (ISEEIE 2021), February 19-21, 2021, Seoul, South Korea*. ACM, New York, NY, USA, 6 pages.

1. INTRODUCTION

Building work teams is a difficult task for a human resource manager (HRM) in that it needs to take into account both the competencies and the relationships between people. These relationships are indeed as much important to work harmoniously together as their competencies. In collaborative work, the participants share a common objective whose success depends on, among others, the quality of the collaborative tasks and on the individual gratefulness. Most of the time, the social trust level between people characterizes these relationships,

which can vary from distrust to trust. [1] consider that a leader-follower relationship between people implies the association of both concepts: vulnerability and trust, and especially in situations where security is prominent. In our research work, we attempt to study this association in situations without hierarchical relationships, but where potential conflicts can occur.

Intending to provide the HRM with a graph of people who could potentially work altogether, we exploit both transitivity and reciprocity of the trust relationships. In other terms, we would like to broaden and to consolidate the graph around people by exploiting respectively the FOAF (friend of a friend) feature and the mutual trust level.

The problem we study in this paper is can we efficiently predict the actual trust values between the users by relying on declared ones?

In the upcoming section, the trust concept is defined according to the scientific literature. In the following section, scientific issues and research questions are presented. In the third section, empirical work with a well-known game allows us to evaluate the link between trust and vulnerability. The last section presents the conclusion and future works.

2. TRUST

In virtual environments, interpersonal trust is a complex concept which is influenced by many factors such as the history of interactions, the similarity in preferences or personal background, the reputation, etc. Trust is primarily subjective in that it underlies inherently a personal opinion about someone in a particular context. Trust is also dynamic and usually non-monotonically changed with time.

The concept of trust is the subject of many definitions. [2] makes a compilation of 72 definitions used in different disciplines. For instance, [3] define trust as the willingness to rely on a reliable person, and [4] define it as an expectation of mutually acceptable behavior.

As trust is an interpersonal concept, social graph topology where the nodes represent people, is considered as the basis of trust computation in most recent models. There are techniques to exploit this information like social network analysis: degree, centrality, and clustering coefficient. Trust between people may be global (n-1 cardinality) and assimilated to a reputation, or local (1-1 cardinality) and relative to interactions between them. Both of them may be defined with numerous models: Advoga, Eigen, O'Dontrust models for the global trust, and Moletrust, Tidaltrust, Appletrust, Abdultrust, Marchtrust, O'Dontrust (both global and local), Bitrellitrust and LSubjtrust for local trust [5]. Most of the computational representations reflect the trust asymmetry by using an oriented graph. [6] provides the following definition of trust: "Alice trusts Bob if she commits to an action based on a belief that Bob's future actions will lead to a good outcome". The transitivity is an important characteristic of

trust and is considered as a base for trust calculation in many trust models. However, trust is not perfectly transitive and degrades along a chain of acquaintances. We seek to show in this research if the transitivity of trust makes sense.

The trust-aware recommendations systems generally rely on an oriented and weighted trust graph and use various metrics for trust. Generally, there are several ways of defining the neighboring in the graph: 1) with the users' similarities matrix, by using the Pearson correlation coefficient for example; 2) with the matrix of the local trust measurements (e.g. MoleTrust [7] for local trust metrics and PageRank [8] for global trust metrics); 3) the combination of both techniques. As the participants of our study do not use any recommender system, we choose the second technique. Trust may be declared explicitly by the users themselves, or deduced from their activities when the context is too sensitive from a relational point of view (in a work team for instance). It is worth noting that trust can not be defined exhaustively in a computational system, and especially because exogenous factors must be considered. However, [5] shows that useful results may be produced by utilizing only information already provided by the users themselves. Our approach is then complementary as we utilize both the declared trust levels and the trust levels which are deduced from their past activities using trace analyses.

Trust is a concept that is defined differently in management, marketing, psychology, and sociology fields. However, the trust concept is commonly associated with the vulnerability one as we can consider that trust consists of sharing the control of our private sphere. [1] confirm that vulnerability is essential for trust, even whether the link between both of them is not still well-defined. In our study, the participants have to make pairs to carry out specific work. In parallel, they can express their trust levels toward the other members through a confidential questionnaire. As the trust concept is not explained to the participants, they decide by themselves the meaning they attribute for trust, and we try to understand their meaning with the results of our experiment. In our study, we postulate that trust deals with hard skills (trade-oriented skills) or soft skills (behavior-oriented skills) depending on the context of work and, in particular, on the coupling level of the work the participants have to carry out.

3. DECLARED TRUST

[9, 10, 11] underline the inherent weaknesses of the recommender systems based on the collaborative filtering, due to the lack of data to measure similarities, and to the risks of fake users' profiles generating. They suggest exploiting declared information by each user about the trustworthiness of the other users. In our experiment, all participants declare generalized trust towards others, without knowing anything about the future collaborative activities they will do. It is worth noting that this kind of trust is limited to small groups, where all members know each other. For large groups, it would be necessary to calculate trust indirectly. [12] highlights that this goal can be reached through the social capital of each member, which is defined as "the ability to secure benefits through membership in networks and other social structures" or, more generally, "resources embedded in networks". The link between trust and social capital is interesting in that the latter is measurable. For instance, social capital can be the average weekly time spent in a volunteer group. This link between both concepts is widely accepted by researchers and gives us insight into the possibility of measuring trust indirectly in larger groups focused on social services, where social relations are based on trust.

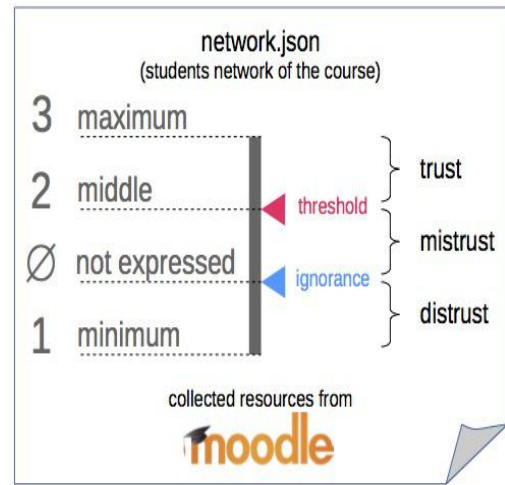


Figure 1. Assumption of the users' Trust Meaning.

In our experiment, participants, who belong to a group of 59 students, may express trust towards others through four values: 0 means "not expressed", 1 means "minimal trust", 2 means "middle trust" and 3 means "maximal trust" [13]. As no meaning of the trust levels has been provided to the users, we distinguish the results associated with the maximal trust link which should not be ambiguous, and those associated with the minimal trust links could be considered as mistrust or distrust. As we do not know the value of the threshold which separates trust and mistrust, we do not take into account the middle trust links in the experiment. Figure 1 illustrates the assumption of the users' trust meaning and our experiment is set out to evaluate, among others, its validity. In the experiment, there are 3422 ($59 * 59$) potential declarations. Table 1 shows the distribution of trust levels (maximum, middle, minimum or not declared). In 45% of cases, the students do not declare a trust level.

3.1. Transitivity of Declared Trust

In most of the research works about trust metrics, the transitivity phenomenon is exploited by the propagation algorithms of trust [14]. A trust-aware recommender system is supposed to provide the applicant a broader mapping than this only of his/her relationships. The trust level defined during the trust statement may be used to predict, by transitivity, the trust level beyond the direct relationships (FOAF) [15]. The resulting trust propagation allows to broad of the users' social network and thus suggests them new resources. For example, MoleTrust of [7] is a local trust metric that enables to create of a tunable trust propagation at a various distance.

3.2. Reciprocity of Declared Trust

As it has been mentioned before, vulnerability and trust are closely linked given that trust corresponds to a positive expectation of receiving something back from the counterpart. Some users may attempt to rely on such users they trust, but without being assured of the reciprocity. An oriented and weighted trust graph contains generally hubs, which are nodes with either the highest reputation or the huge production. Even it is oriented, the graph presented to the users does not display the arrows not to reveal the personal trust statements. However, a trust-aware recommender system can use this information to regulate potential recommendations.

In our experiment, Table 2 shows for each student A , the possible declared trust of another student B with respect to A . Several

remarks can be formulated: 1) In the case where A declares maximal trust in B , the table shows a decrease in the declared trust of B face to A from 39% for the maximal, and to 8% for the minimal. 2) In the case where A declares minimal trust in B , the latter declares maximal trust in A in only 6% of the cases B , which corresponds to a certain (negative) reciprocity.

This result shows the existence of reciprocity for the declared trust. However, it is difficult to measure its degree which is far from 100%. We ignore both middle trust and not declared trust, because we do not know how to interpret them.

Table 2. Reciprocity of declared trust.

A 's declared trust in B	B 's declared trust in A			
	Maximal	Middle	Minimal	B not declare trust
Maximal	198, 39%	119, 24%	40, 8%	136, 27%
Minimal	40, 6%	140, 23%	120, 20%	293, 49%

3.3. Trust vs. Profitability

For the economists, the membership in voluntary associations defines the associative social capital. According to [12], associative social capital is originated by participation in social networks, where the members, who are the nodes, benefit from the interconnections with the other nodes. He postulates that cooperation leads to a better social and individual outcome like it is usually observed in the prisoner's dilemma. The player's choice is affected by his beliefs about the counterpart's belief about his choice.

4. TRUST CHALLENGE, ACTUAL TRUST

4.1. General Context of Experimentation

This experiment was inspired by Albert W. Tucker's prisoner's dilemma. In this context, the real trust, which is given to a person and called the "actual trust", plays a key role. Our goal in this study is to confront this "actual trust" with the previously "declared trust".

We provide a game to a group of 59 students. Students often do practical work in pairs and they obtain the same score (out of 20 points). Our experiment consists of a game where we propose to a pair to participate in a "Challenge". This activity does not affect their grades. Both students can select whether s/he "shares" or "does not share" a hypothetical note. The possible results of a "challenge" are: a) if both members of the pair decide to "share", each will obtain the score of 10/20; b) If both decide "do not share", each will obtain the score 0/20; c) If one decides "do not share" and the other "share", the first will get 20/20 and the second 2/20. The choices are anonymous and asynchronous. There is no communication between the participants and all students had a 10 days deadline to participate in the challenges which were proposed to them.

Figure 2 shows the user's home page of our experiment. In the middle part of the figure, on the left side, there are the names of the students with whom a challenge can be initiated and on the right side, the names of the students with whom a challenge can be completed. In the lower part, the user can see a history of the challenges in which s/he has already participated.

Table 1. Overall Declared trust.

Declared trust	number	percent
Maximal	493	14%
Middle	841	24%
Minimal	593	17%
Non declared	1554	45%

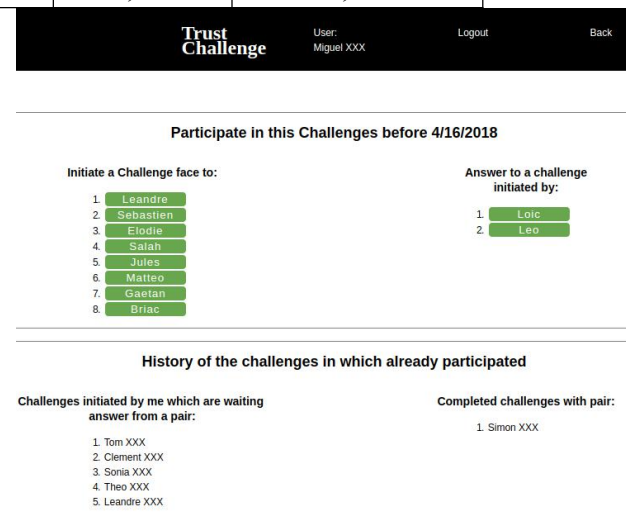


Figure 2. User Home Page of Trust Challenge.

Figure 3 shows one challenge. The user can select "share" or "do not share" with his/her pair. The choice "share" can be considered as a trust given to a pair. Whereas the choice of "do not share" can be interpreted as a lack of trust.

Figure 4 is shown at the end of the game when the deadline for participating in challenges is over. The users can see the history of their challenges, their obtained average score, and the overall scores.

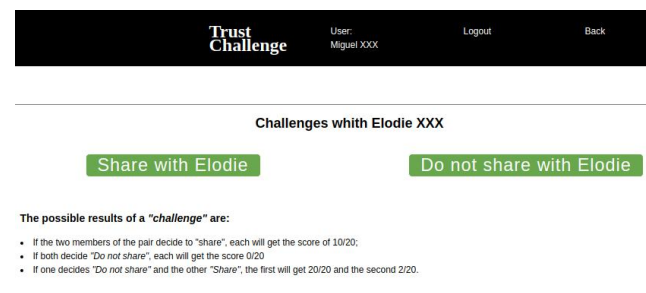


Figure 3. One Challenge.

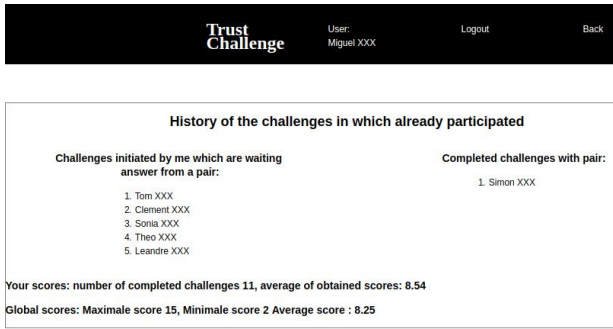


Figure 4. User Results.

4.2. Pair formation

In the experiment, 302 challenges have been proposed, i.e. 604 potential responses. The number of challenges per student on average is 10.2.

Table 3. Completed Challenges.

Number of completed challenges	number	percent
Total	199	100%
Challenges where both students selected "share"	94	47%
Challenges where both selected "do not share"	39	19%
Challenges where one selected "share" and the other "do not share"	66	33%

4.4. Challenge's Responses vs the Declared Trust

In Table 4, the individual responses of the students are considered without taking into account the possible response of

Table 4. A Responses vs Declared Trust.

A's declared trust	A's responses			A not response
	number	"Share"	"Do not share"	
Maximal	205	157, 76%	48, 23%	33
Maximal transitive	156	98, 62%	58, 37%	50
Minimal	121	51, 42%	70, 57%	39

Several remarks can be formulated:

1) The numbers of "share" responses in the case of a maximal declared trust level (76%) and the case of a minimal declared trust level (42%) confirm the intuition of a correspondence between the declared trust level and the actual trust level. The minimal declared trust level can be interpreted as a lack of trust or distrust, while maximal declared trust level does not correspond to a 100% actual trust. It's not a blind trust.

2) In the case of a maximal transitive trust, the number of "share" responses (62%) consolidates the reality of the notion of transitivity for trust. Incidentally, we note in this case an increase

As previously, we will call A and B the two students who form a pair during a challenge.

To be able to compare the results of the challenges (actual trust) with the declared trust, we have retained the following criteria to form the pairs which will be proposed to the students: 1) Binomials where a mutual maximal trust level has been declared. 2) Binomials where a maximal trust level has been declared by third parties, that is to say, maximal transitive trust 3) Binomials where asymmetrical trust levels have been declared, one with maximal trust level and the other with minimal trust level. 4) Binomials where a mutual minimal trust level has been declared.

4.3. Challenges Results

At the end of the gaming period, out of 302 proposed challenges, 199 were completed (both members of the pair responded). Table 3 gives a summary of the completed challenges. We can notice that in almost half of the completed challenges, both students select "share".

their peer. The table shows the A 's responses according to three cases of the declared trust level of A in a pair: maximal, maximal transitive and minimal trust. In each case, for a challenge A can select: 1) "Share", 2) "Do not share", or 3) not to the response.

in the number of "non-responses". Students tend to participate less in challenges involving other students for whom they have not previously declared the trust level.

It can be concluded that the declared trust is in line with the actual trust given during the challenges and the notion of transitivity of trust makes sense.

4.5. Reciprocity of Actual Trust

It is interesting to verify if an actual trust is usually mutual. Table 5 shows the possible responses of B compared to A 's responses without taking into account the declared trust level.

Table 5. Reciprocity of Actual Trust.

A's responses	A "share"			A "do not share"		
	B's response			B's response		
	nb	"Share"	"Do not share"	nb	"Share"	"Do not share"
398	254	188, 74%	66, 25%	144	66, 45%	78, 54%

We remark that globally there is a reciprocity in the responses. In 74% of cases, both students decide to "share". That is a quite

high percentage, even though the responses are anonymous and that the game encourages the "treachery". In the opposite case,

when A selects "do not share", only in 45% of cases B selects "share". The averages obtained clearly show that the reciprocity of actual trust makes sense.

However, it does not make sense to compare the percentages of reciprocity between actual trust and declared trust. Indeed, the calculation of this percentage for the actual trust only takes into account the set of responses, while the reciprocity percentage of the declared trust takes into account all the members of the group, regardless of whether they declare a trust.

5. TRUST AND RECOMMENDER SYSTEMS

According to the recurring lack of data in the recommender systems based on collaborative filtering, [14, 11, 16] underline both the growing interest in taking into account the trust and distrust concepts in these systems and the difficulty to grasp these concepts and especially distrust. [10] propose a rank method that learns about friends' trust and foes' distrust to move the recommended items closer to, respectively away from, the applicant. [17] show how a social graph data can increase the users' acceptance of the results of the recommender systems and underline that the trust-aware recommender algorithms allow all explanation styles (human, features, items, and their combinations). In the context of recruitment, where relationships between members of a workgroup are important, mutual trust is a significant criterion in recommender systems. The results of our study show that maximal trust is globally reciprocal and that minimal trust corresponds to a certain (negative) reciprocity. In Figure 5, the edges are red when the maximal actual trust levels match the maximal declared ones. The numerous red edges of the graph convey us to think that declared trust can be exploited to predict actual trust using reciprocity and transitivity. To extend the graph to larger groups, we use the transitivity of trust to enlarge knowledge about the members' trustworthiness of small groups to wide groups where people do not know each other.

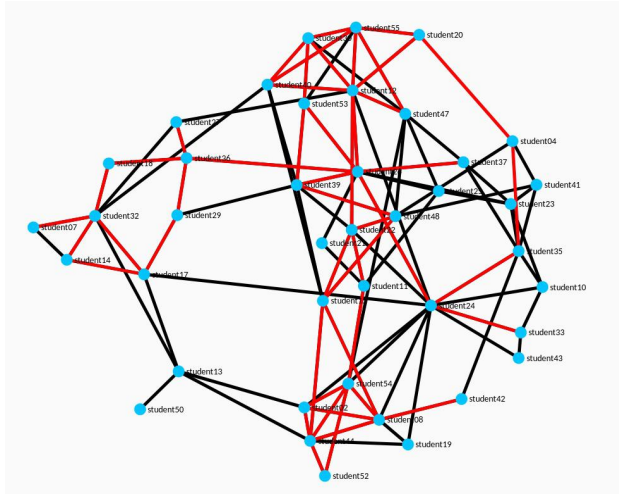


Figure 5. Declared vs. Actual Trust for a Recommendation.

6. CONCLUSION

The game "Trust Challenge" allowed to explore the notion of trust, and to highlight that declared trust is in line with actual trust. The results of the experiment prove the reality of the reciprocity and the transitivity for both declared and actual trusts. As far as the trust metrics are concerned, if both maximal and minimal trust levels may be easily interpreted, both middle and

not declared trust levels are ambiguous. This choice avoids the problem of the threshold definition between trust and distrust.

To consolidate our results, other studies involving sociologists and a much larger study population are needed. Nevertheless, our study confirms the interest of using the concept of trust as one of the criteria for recommending people for the formation of work teams and the real meaning of the reciprocity and the transitivity of trust.

7. MATERIALS AND METHOD

7.1. Objectives Definition

Our research work on the relevance of declared trust for recommending profiles of competences is evaluated in this paper by an experiment with students. Another experiment on the use of trust with researchers and a prototype of the recommender system is currently conducted in our laboratory. The present experiment has been conducted in less than two weeks, and the target users are 59 students who know each other. The studied entities are individuals who have declared their trust levels towards the others, one month before. Besides that, the participants' profiles of competences are based on their hard skills in HTML/JavaScript programming language and on their self-declared soft skills.

7.2. Existing Data Inventory

The group of 59 students is composed of 12 girls and 47 boys who are 20 years old on average. They are living in the same country and they are talking the same language. They know each other and study together for 4 months. Each participant has declared privately using a questionnaire his/her trust level towards the other participants as s/he wished (nothing, minimal, middle, or maximal level). In the same way, they have declared through a questionnaire their soft skills with thirty-three criteria: attentive/inattentive, who listens to criticism/susceptible, adaptable/rigid, kind/cranky, autonomous/dependent, etc. To guaranty the privacy and the legality of this research work, the researchers and the students have cosigned an agreement before participating in the experiment, which stipulates that the former engage themselves not to publish nominative results.

7.3. Data Collect

Both trust and skills information stems from digital questionnaires and the resulting matrices are stored in CSV (Comma-Separated Values) files. The game setting, like pairs definition, depends on the declared trust levels as explained in a previous part. When the game is over, the results have been stored in a database to be analyzed afterward. The results of the experiment stem from the traces of interaction with the game through software instrumentation.

7.4. Data Exploration and Preparation

Before analyzing data, personal information is made anonymous following the aforementioned agreement. For the trust information, we do not take into account the middle trust links in the experiment, because we do not know how the users interpret this trust level: trust or mistrust? We use the BEATCORP platform, which is a trace-based system, to exploit the corpora of data before creating the graphs with the JSON format. The graph presented Figure 5 has been displayed with our visualization tool.

7.5. Population Segmentation

An entire class of students has been selected to form a homogeneous group in terms of age and knowledge. All the

students are in their first year at the university and know each other for only 4 months.

REFERENCES

- [1] P. D. Romeike, M. Hofeditz, A.-M. Nienaber, Vulnerability and trust in leader-follower relationships, *Personnel Review*, vol. **44**, pp.567-591, (2015)
- [2] S. Castaldo, Trust in Market Relationships, p.320, (2007)
- [3] C. Moorman, G. Zaltman; R. Deshpande, Relationships between Providers and Users of Market Research: The Dynamics of Trust within and between Organizations, *Journal of Marketing Research*, vol. **29**, pp.314-328, (1992)
- [4] M. Sako, S. Helper, Determinants of trust in supplier relations: Evidence from the automotive industry in Japan and the United States, *Journal of Economic Behavior & Organization*, vol. **34**, pp.387-417, (1998)
- [5] J. Golbeck, Trust and Nuanced Profile Similarity in Online Social Networks, *ACM Trans. Web*, vol. **3**, pp.12:1–12:33, (2009)
- [6] J. Golbeck, Computing and Applying Trust in Web-based Social Networks, (2005)
- [7] P. Massa, P. Avesani, Trust Metrics on Controversial Users: Balancing Between Tyranny of the Majority, *International Journal on Semantic Web and Information Systems (IJSWIS)*, vol. **3**, pp.39-64, (2007)
- [8] L. Page, S. Brin, R. Motwani, T. Winograd, The PageRank Citation Ranking: Bringing Order to the Web. (1999)
- [9] P. Massa, P. Avesani, Trust Metrics in Recommender Systems Computing with Social Trust, *Human-Computer Interaction Series*, pp.259-285, London, (2009)
- [10] D. Rafailidis, F. Crestani, Learning to Rank with Trust and Distrust in Recommender Systems, *Proceedings of the Eleventh ACM Conference on Recommender Systems (RecSys '17)*, pp.5–13, New York, NY, USA, (2017)
- [11] R. Forsati, I. Barjasteh, F. Masrour, A.-H. Esfahanian, H. Radha, PushTrust: An Efficient Recommendation Algorithm by Leveraging Trust and Distrust Relations, *Proceedings of the 9th ACM Conference on Recommender Systems (RecSys '15)*, pp.51–58, New York, NY, USA, (2015)
- [12] M. Migheli, Assessing Trust Through Social Capital? A Possible Experimental Answer, *American Journal of Economics and Sociology*, vol. **71**, pp.298-327, (2012)
- [13] C. Courtin, M. Tomasena, A benchmarking platform for analyzing corpora of traces: the recognition of the users' involvement in fields of competencies. *Proceedings of the 3rd IEEE/ACM International Conference on Big Data Computing, Applications and Technologies*, Shanghai, China, (2016)
- [14] P. Gao, H. Miao, J. S. Baras, J. Golbeck, STAR: Semiring Trust Inference for Trust-Aware Social Recommenders, *Proceedings of the 10th ACM Conference on Recommender Systems (RecSys '16)*, pp.301–308, New York, NY, USA, (2016)
- [15] G. Alexandridis, G. Siolas, et A. Stafylopatis, Enhancing social collaborative filtering through the application of non-negative matrix factorization and exponential random graph models, *Data Min Knowl Disc (DMKD)*, vol. **31**, no4, pp.1031- 1059, (2017).
- [16] H. Ma, M. R. Lyu, I. King, Learning to Recommend with Trust and Distrust Relationships, *Proceedings of the Third ACM Conference on Recommender Systems (RecSys '09)*, pp.189–196, New York, NY, USA, (2009)
- [17] A. Papadimitriou, P. Symeonidis, Y. Manolopoulos, A generalized taxonomy of explanations styles for traditional and social recommender systems, *Data Min Knowl Disc (DMKD)*, vol. **24**, pp.555-583, (2012)