This is the accepted manuscript of the article that appeared in final form in **Neurocomputing** 166 : 1-7 (2015) , which has been published in final form at http://dx.doi.org/10.1016/j.neucom.2014.10.099. © 2015 Elsevier under CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

Reputation features for trust prediction in social networks

J. David Nuñez-Gonzalez (1), Manuel Graña (1), Bruno Apolloni (2)

(1) UPV/EHU, (2) University of Milano

Abstract

Trust prediction in Social Networks is required to solve the cold start problem, which consists of guessing a Trust value when the truster has no direct previous experience on the trustee. Trust prediction can be achieved by the application of machine learning approaches applied to reputation features, which are extracted from the available Trust information provided by witness users. Conventional machine learning methods work on a fixed dimension space, so that variable size reputation information must be reduced to a fixed size vector. We propose and give validation results on two approaches, (1) a naïve selection of reputation features, and (2) a probabilistic model of these features. We report experimental results on trust prediction over publicly available Epinions and Wikipedia adminship voting databases achieving encouraging results.

. Introduction

Trust has been a traditional subject of study in four different areas of knowledge, namely social psychology [1], philosophy, economics and market research [4], however it is increasingly becoming a subject of research in technological domains, such as *ad hoc* networks [2], [5], [7], Medical Sensor Networks [14], Industrial Digital Ecosystems [9], and e-commerce [18]. There have been some efforts to produce mathematical definitions of trust [22], [10], however intuitive informal definitions, such as “the degree of subjective belief about the behaviors of (information from) a particular entity” [8], or “the expectation that a service will be provided or a commitment will be fulfilled” [15], are convenient for the purposes of this paper. Trust research can be organized [3] in four major areas: (1) policy-based trust, (2) reputation based trust, (3) general models of trust and (4) trust information resources, related with the following applications: networking, semantic web, computational models, game theory and agents, software engineering and information resources. The present paper deals with trust in a Social Network context.

In Social Networks, trust is built from experience along a feedback process. The truster makes decisions based on trust built on the trustee part. Positive or negative results will maintain, increase or decrease the trust value. The cold start problem rises when there is no previous experience about the trustee behavior. Then, there is a need to predict the trust value [12] from indirect information, that is, from reputation information obtained from third party witness. Trust prediction can be formulated as a classification problem, where feature vectors are computed from the reputation information extracted from the

1 http://www.epinions.com/.
2 http://www.trustlet.org/wiki/Extended_Epinions_dataset.
3 http://snap.stanford.edu/data/wiki-Elec.html.
4 http://www.ehu.es/ccwintco/index.php/GIC-experimental-databases
5 http://www.cs.waikato.ac.nz/ml/weka/.
6 http://www.sands-project.eu/.

network. Although the trust relation between users is not transitive [7], [11], [21], reputation can be accepted as the best guess information that can be used to predict the trustworthiness of a trustee. In this paper we discuss specific reputation features that can be extracted from the social network for application of conventional machine learning classifiers to trust prediction, providing experimental results over benchmark databases.

The paper is organized as follows: Section 2 describes the experimental databases and the feature extraction processes applied to obtain the reputation feature datasets. Section 3 gives the experimental results. Finally, Section 4 gives some conclusions and directions of future research work.

2. Experimental databases and reputation features

2.1. The original databases

We use two databases for experimentation which have been extracted from the Epinions and Wikipedia web sites and published for experimentation in the repository built by the Stanford Network Analysis Project http://snap.stanford.edu/

Epinions database: The Epinions site[1] is a social webservice where users provide reviews of products of any kind, ranging from music up to perfumes or construction hardware. These reviews are the base for the establishment of trust relations between users. Trust is a binary variable taking values in

: a truster user can choose to trust (1) or distrust (−1) another, the trustee. Negative trust values are not published in the web service, but the anonymized dataset provided for experimentation, which is available to the public,[2] contains also negative Trust values. This dataset has 841,372 data samples. Each sample is a triplet

composed of two user indexing numbers (no personal data of any form is included) and the binary Trust value of the first user on the second user. Therefore, Trust relations define a directed graph, with weighted edges. Regarding class distributions, the database is unbalanced: 85.3% of instances are positive trust (717,667 triplets), while 14.7% are negative trust instances (123,705 triplets). This data base has been used previously to perform computational experiments of Trust models [19], [20].

Wikipedia database: Wikipedia is a free encyclopedia built by crowd-sourcing efforts from volunteers around the world. A small part of Wikipedia contributors are administrators, who are users with access to additional technical features that aid in maintenance. In order for a user to become an administrator a Request for adminship (RfA) is issued and the Wikipedia community via a public discussion or a vote decides whom to promote to adminship. The actual database[3] employed in this paper has the following format:

- •E: did the elector result in promotion (1) or not (0).
- •T: time election was closed.
- •U: user id (and screen name) of editor that is being considered for promotion.
- •N: user id (and screen name) of the nominator.
- •V: vote(1: support, 0: neutral, -1: oppose) user_id time screen_name.

1 http://www.epinions.com/.
2 http://www.trustlet.org/wiki/Extended_Epinions_dataset.
3 http://snap.stanford.edu/data/wiki-Elec.html.
4 http://www.ehu.es/ccwintco/index.php/GIC-experimental-databases
5 http://www.cs.waikato.ac.nz/ml/weka/.
6 http://www.sands-project.eu/.

For the work in this paper, the trust triplet (A, B, t_ab)

is built from three attributes: voting user, voted user and the vote value. Regarding the vote value, we are interested in two out of three possible vote values: 1 (support) and −1 (oppose). We ignore the vote "0". For this reason, we reorganize the database as follows: each row has the three attributes mentioned before: [userA, userB, vote]

In summary, we obtain a social network trust database containing 103,591 instances (78.83% for class "1" and 21.17% for class "−1"). We will make feature extraction from this database.

Previous work on this database has been reported in [17], [16]. In the first work they investigated two theories of signed social networks: balance and status. These two theories make different predictions for the frequency of different patterns of signed links in a social network. In the second work, they investigated some of the underlying mechanisms that determine the signs of links in large social networks where interactions can be both positive and negative.

2.2. Feature extraction

From the original databases, we perform feature extraction in two different ways to obtain the reputation feature datasets, which will be published at the group's website[4] for independent third party assessment of results and experimentation. From the original database of triplets, we build several databases of reputation features, consisting of the observation of the Trust values of related users. Each database entry is composed of a feature vector of specific dimension and the trust value to be predicted. Let us introduce some common notation: For each triplet (A, B, t_{AB}) we construct a list of witness users, $L_{AB} = \{C|(C,A, t_{AB}) € D \wedge (C,B, t_{CD}) € D\}$ where D denotes the original database of triplets. The node *A* queries its trusted peers C_i about their trust on target trustee *B*. The computation of the feature extraction took several days due to the large database sizes and the need to perform exhaustive examinations. We did not record computation times precisely.

2.2.1. Raw reputation vectors of fixed dimension

Fig. 1 illustrates the reputation features provided by the witness and that are used to achieve the construction of the feature vector for a given (A,B) pair. Machine learning classifiers are often working in a data space of specific dimension, so that feature vectors are of fixed dimension. The set of witness that provide the reputation values may have any size. To solve this problem, a naive approach to the construction of the reputation database is as follows: Given feature vector dimension *d*, we discard the triplet (A,B, L_{AB}) if | t_{AB} |<d . If | L_{AB} | > d, we perform a random selection of *d* witness nodes *C* obtaining L^*_{AB} such that | L^*_{AB} |. The input/output pair (X,Y) in the reputation feature database corresponding to triplet (A,B, t_{AB}) is constructed such as X = { t_{CB} | C € L^*_{AB} } and Y= t_{AB}. We have considered *d*=3 and *d*=10 in the present paper, in other words, the input data *X* is a matrix of 3 or 10 columns.

1 http://www.epinions.com/.
2 http://www.trustlet.org/wiki/Extended_Epinions_dataset.
3 http://snap.stanford.edu/data/wiki-Elec.html.
4 http://www.ehu.es/ccwintco/index.php/GIC-experimental-databases
5 http://www.cs.waikato.ac.nz/ml/weka/.
6 http://www.sands-project.eu/.

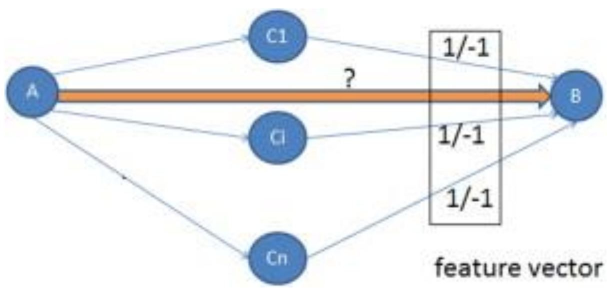

Fig. 1. Unconditional reputation features of witnesses { C_i } on the trustee B.

2.2.2. Probabilistic feature vectors

Another approach to obtain fixed size feature vectors is to consider some functions on the variable size reputation sets obtained from the witness sets, i.e. some statistics. In this paper we consider probabilistic features which are the conditional probabilities of the witness trust on the trust of the truster on the witness. They are computed as follows: For each set of witness L_{AB} we differentiate the following sets:

$$L_{CB}^{++} = \{C \in L_{AB} | t_{AC} =+ 1 \wedge t_{CB} =+ 1\}, L_{CB}^{+-} = \{C \in L_{AB} | t_{AC} =+ 1 \wedge t_{CB} = -1\}, L_{CB}^{-+} = \{C \in L_{AB} | t_{AC} = -1 \wedge t_{CB} =+ 1\}, L_{CB}^{--} = \{C \in L_{AB} | t_{AC} = -1 \wedge t_{CB} = -1\}.$$

These sets correspond to the possible kinds of paths linking the truster to the trustee through some witness. Fig. 2 illustrates these four possible paths. Then we can compute the following conditional probabilistic features of the reputation feature set:

$$P\left(t_{CB} =+ 1 \middle| t_{AC} =+ 1\right) = \frac{|L_{CB}^{++}|}{|L_{AB}|}, P\left(t_{CB} = -1 \middle| t_{AC} =+ 1\right) = \frac{|L_{CB}^{+-}|}{|L_{AB}|},$$
$$P\left(t_{CB} =+ 1 \middle| t_{AC} = -1\right) = \frac{|L_{CB}^{-+}|}{|L_{AB}|}, P\left(t_{CB} = -1 \middle| t_{AC} = -1\right) = \frac{|L_{CB}^{--}|}{|L_{AB}|}.$$

[1] http://www.epinions.com/.
[2] http://www.trustlet.org/wiki/Extended_Epinions_dataset.
[3] http://snap.stanford.edu/data/wiki-Elec.html.
[4] http://www.ehu.es/ccwintco/index.php/GIC-experimental-databases
[5] http://www.cs.waikato.ac.nz/ml/weka/.
[6] http://www.sands-project.eu/.

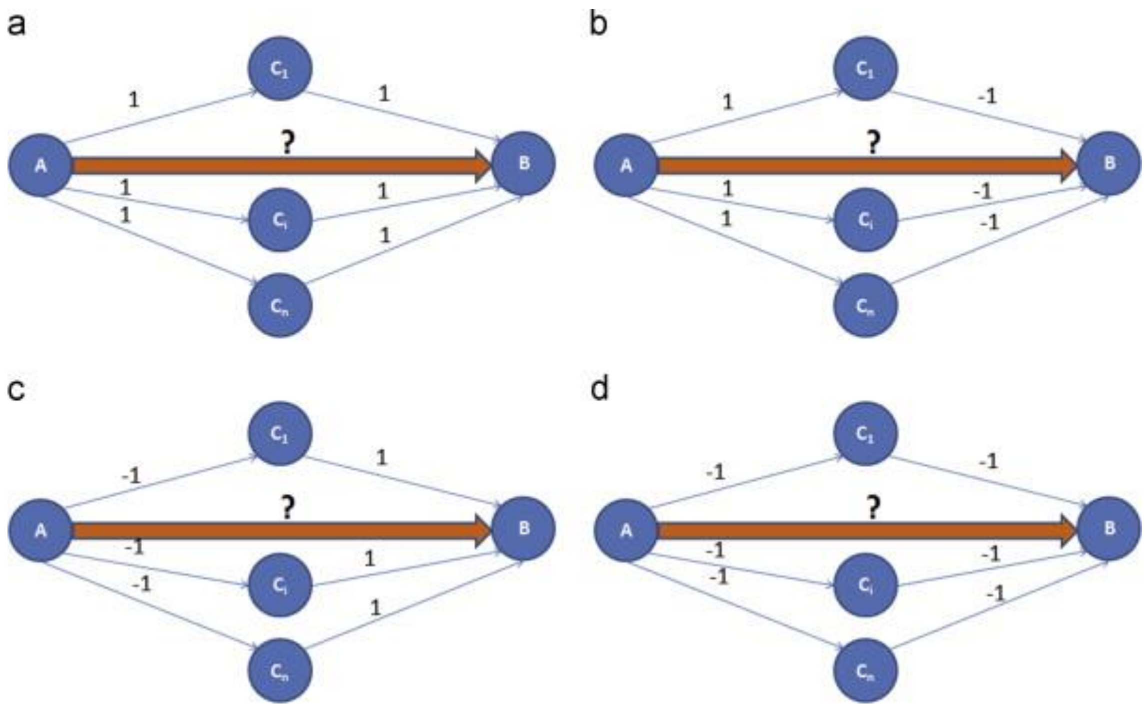

Fig. 2. The four possible paths from truster *A* to trustee *B* through a witness *C* according to the trust labels used for the probabilistic reputation features.

Therefore, we obtain a feature vector of low dimension (i.e., 4) that summarizes the trust information on the witness set. After calculation of the probabilistic feature vectors in the case of Wikipedia, we remove instances with NaN values, so that the final feature dataset has 75,760 instances (78.45% of class “1”, and 21.55% of class “−1”). From the Epinions database, we obtain a dataset with 547,694 instances (89.01% of class “1”, and 10.99% of class “−1”), so that coverage of the Epinions database is 100% in the experiments.

3. Experimental work and results

Machine learning classification algorithm implementations are obtained from Weka.[5] Specifically, we have tested Naive Bayes (NB), Multilayer Perceptron (MLP), Radial Basis Function classifier (RBFC) and network (RBFN), Support Vector Machine (SVM), AdaBoost, and decision tree algorithms JRip and J48. Computational experiments consist of 10-fold cross-validation over the whole databases. We report overall average accuracy (OA), and *per* class recall (R) and precision (P) measures. The two classes considered are Trust (+1) and Notrust (−1).

1 http://www.epinions.com/.
2 http://www.trustlet.org/wiki/Extended_Epinions_dataset.
3 http://snap.stanford.edu/data/wiki-Elec.html.
4 http://www.ehu.es/ccwintco/index.php/GIC-experimental-databases
5 http://www.cs.waikato.ac.nz/ml/weka/.
6 http://www.sands-project.eu/.

3.1. Results on raw reputation features

In the first experiment, we build classifiers over raw reputation feature vectors of static size. Feature vectors are composed of the trust (1) and distrust (-1) values of the witness users towards the trustee. The class distributions are very imbalanced, which account for the poor recall and precision results of the Notrust class, and the corresponding low OA. We also report results after the application of database balancing techniques, i.e. SMOTE described below, which improve the performance over the Notrust class.

SMOTE: Synthetic Minority Over-sampling Technique (SMOTE) [6] consists in the generation of new samples of the minority (less frequent) class in order to obtain a more balanced representation of the classes. Instead of performing a re-sampling with replacement from the original database, which only introduces repetitions of the already sampled points in the feature space, SMOTE performs interpolation processes in order to generate new sampling points in feature space. Mere replication of sampling points do not alter the decision boundary. SMOTE works in feature space by the following process for each minority class sample (or a random subset of them): X_0:

1. Select its *k* minority class nearest neighbors $N_k(\mathbf{x}_0)$.
2. Draw the line between each $\mathbf{x}_i \in N_k(\mathbf{x}_0)$ and $\mathbf{x}_0$.
   (a) compute the new sample picking a random position in this line (random linear interpolation):

   $$\mathbf{x}_i^* = \alpha\mathbf{x}_0 + \left(1-\alpha\right)\mathbf{x}_i,$$

   where $\alpha \sim U(0,1)$ is a random number between 0 and 1.
3. Add the generated samples to the minority class training data.

This process can be tuned specifying the number of nearest neighbors. SMOTE can be used in combination with majority class under-sampling (removing samples). Notice that SMOTE may “fill the gaps” in data distributions that show disperse connected regions.

3.1.1. Results

Table 1, Table 2, Table 3, Table 4, Table 5 provide results on the Epinions and Wikipedia datasets of raw reputation features of vector dimension 10 and 3. The effect of database imbalance is stronger for the Wikipedia database. Table 1, Table 3 present the results without the application of the SMOTE preprocessing. The OA values are heavily influenced by the Trust class success, in Epinions the OA average for 10 and 3 features (there is not significant difference due to feature size) is 93% in Table 1, and 90% in the Wikipedia database. In the latter, results for Notrust class are zero for all classifiers and feature sizes. The application of SMOTE does not improve the OA, in fact it goes down to 89% in Epinions (Table 2) and to 76% in Wikipedia (Table 4), however there is a clear improvement on the Notrust classification in recall and precision of Notrust which can compensate the worsening for Trust if the cost of false Trust is much higher than that of false Notrust. Additional iterations of SMOTE do not improve the OA, and continue the

1 http://www.epinions.com/.
2 http://www.trustlet.org/wiki/Extended_Epinions_dataset.
3 http://snap.stanford.edu/data/wiki-Elec.html.
4 http://www.ehu.es/ccwintco/index.php/GIC-experimental-databases
5 http://www.cs.waikato.ac.nz/ml/weka/.
6 http://www.sands-project.eu/.

decrease/increase of recall and precision for the Trust/Notrust class, as shown in Table 5 where Notrust reaches 73% recall for 10 features and 55% recall for 3 features. The effect of feature size is also greater for Wikipedia than for Epinions database.

Classif.	10 features					3 features				
	OA	Trust		Notrust		OA	Trust		Notrust	
		R	P	R	P		R	P	R	P
NB	90.02	100.0	90.0	0.0	0.0	90.02	100.0	90.0	0.0	0.0
MLP	93.80	98.8	94.6	49.0	81.5	93.41	99.3	93.7	39.9	87.1
RBFC	93.90	98.9	94.6	49.24	82.7	93.41	99.3	93.8	45.2	86.1
RBFN	93.75	99.5	93.9	41.6	90.8	92.77	98.6	93.7	40.40	75.8
SVM	93.90	99.0	94.5	47.6	84.6	93.44	99.5	93.6	38.6	89.8
AdaBoost	93.43	98.4	94.5	48.5	77.2	93.24	98.2	94.5	48.9	74.6
JRip	93.87	98.8	94.6	49.1	82.3	93.44	99.5	93.6	38.6	89.8
J48	93.86	99.0	94.5	47.6	83.9	93.44	99.5	93.6	38.6	89.8

Table 1. Results of cross-validation experiments on the raw reputation features of the Epinions database without SMOTE preprocessing – 10 and 3 features.

Classif.	10 features					3 features				
	OA	Trust		Notrust		OA	Trust		Notrust	
		R	P	R	P		R	P	R	P
NB	85.77	88.2	94.0	74.7	58.5	90.02	100.0	90.0	0.0	0.0
MLP	90.03	97.8	90.7	54.9	84.9	89.45	97.5	90.4	53.1	82.6
RBFC	90.08	97.6	90.9	56.1	84.0	89.49	97.4	90.4	53.6	82.3
RBFN	89.84	97.3	90.9	56.2	82.1	89.49	97.4	90.4	53.6	82.3
SVM	90.15	98.1	90.6	54.1	86.5	89.49	97.4	90.4	53.6	82.3
AdaBoost	89.74	97.5	90.7	54.8	82.8	89.49	97.4	90.4	53.6	82.3
JRip	90.09	98.0	90.7	54.5	85.7	89.49	97.4	90.4	53.6	82.3
J48	90.12	98.0	90.7	54.5	85.7	89.49	97.4	90.4	53.6	82.3

Table 2. Results of cross-validation experiments on the raw reputation features of the Epinions database after one SMOTE iteration of database balancing – 10 and 3 features.

1 http://www.epinions.com/.
2 http://www.trustlet.org/wiki/Extended_Epinions_dataset.
3 http://snap.stanford.edu/data/wiki-Elec.html.
4 http://www.ehu.es/ccwintco/index.php/GIC-experimental-databases
5 http://www.cs.waikato.ac.nz/ml/weka/.
6 http://www.sands-project.eu/.

Classif.	10 features					3 features				
	OA	Trust		Notrust		OA	Trust		Notrust	
		R	P	R	P		R	P	R	P
NB	90.02	100.0	90.0	0.0	0.0	90.02	100.0	90.0	0.0	0.0
MLP	90.02	100.0	90.0	0.0	0.0	90.02	100.0	90.0	0.0	0.0
RBFC	90.02	100.0	90.0	0.0	0.0	90.02	100.0	90.0	0.0	0.0
RBFN	90.02	100.0	90.0	0.0	0.0	90.02	100.0	90.0	0.0	0.0
SVM	90.02	100.0	90.0	0.0	0.0	90.02	100.0	90.0	0.0	0.0
AdaBoost	90.02	100.0	90.0	0.0	0.0	90.02	100.0	90.0	0.0	0.0
JRip	90.02	100.0	90.0	0.0	0.0	90.02	100.0	90.0	0.0	0.0
J48	90.02	100.0	90.0	0.0	0.0	90.02	100.0	90.0	0.0	0.0

Table 3. Results of cross-validation experiments on the raw reputation features of the Wikipedia database without SMOTE preprocessing – 10 and 3 features.

Classif.	10 features					3 features				
	OA	Trust		Notrust		OA	Trust		Notrust	
		R	P	R	P		R	P	R	P
NB	75.19	81.6	84.7	56.1	50.5	90.02	100.0	90.0	0.0	0.0
MLP	76.86	93.8	79.2	26.4	58.6	75.56	95.1	77.4	17.2	54.0
RBFC	77.04	93.1	79.7	28.9	58.5	75.98	94.8	77.9	20.0	56.0
RBFN	76.87	93.3	79.5	27.9	58.1	75.87	94.3	78.0	20.7	55.03
SVM	76.87	94.0	79.1	25.7	58.9	75.99	96.2	77.3	15.6	57.9
AdaBoost	76.42	95.1	78.2	20.6	58.5	75.93	94.3	78.1	21.0	55.3
JRip	76.40	91.5	79.9	31.2	55.2	75.99	96.2	77.3	15.6	57.9
J48	76.78	94.1	78.9	25.0	58.7	75.99	96.2	77.3	15.6	57.9

Table 4. Results of cross-validation experiments on the raw reputation features of the Wikipedia database after one SMOTE iteration – 10 and 3 features.

1 http://www.epinions.com/.
2 http://www.trustlet.org/wiki/Extended_Epinions_dataset.
3 http://snap.stanford.edu/data/wiki-Elec.html.
4 http://www.ehu.es/ccwintco/index.php/GIC-experimental-databases
5 http://www.cs.waikato.ac.nz/ml/weka/.
6 http://www.sands-project.eu/.

Classif.	10 features					3 features				
	OA	Trust		Notrust		OA	Trust		Notrust	
		R	P	R	P		R	P	R	P
NB	71.31	81.2	73.6	56.5	56.5	90.02	100.0	60.0	0.0	0.0
MLP	71.03	75.8	75.8	63.9	63.9	69.84	79.1	72.9	55.9	64.2
RBFC	71.27	76.1	76.0	64.1	64.2	69.84	79.1	72.9	55.9	64.2
RBFN	70.97	69.1	79.1	73.7	61.5	69.84	79.1	72.9	55.9	64.2
SVM	70.97	70.1	79.0	73.4	61.8	69.84	79.1	72.9	55.9	64.2
AdaBoost	67.46	88.9	67.3	35.4	68.1	67.42	87.1	67.7	38.1	66.3
JRip	71.27	73.2	77.6	68.4	63.1	69.84	79.1	72.9	55.9	64.2
J48	71.25	72.3	78.1	69.6	62.7	69.84	79.1	72.9	55.9	64.2

Table 5. Results of cross-validation experiments on the raw reputation features of the Wikipedia database after two SMOTE iteration – 10 and 3 features.

3.2. Results on probabilistic reputation features

As shown in Table 6, carrying a 10-fold cross-validation experiment over the probabilistic reputation features we achieve performance results close to perfect measured in average overall accuracy (OA), F1score (F1), and area under the ROC (AUC). The differences between the different classifiers are minimal, not significant in the statistical sense (*t*-test). The reason for such spectacular success is the fact that the probabilistic features are greatly discriminant of the classes in the problem at hand, as can be appreciated by inspection of Fig. 3, Fig. 4 showing the class conditional *a priori* distributions of the values of each probabilistic feature, where Magenta corresponds to the Trust class and blue to the Notrust class. In all plots, the separation of classes is very clear making the problem very easy for conventional classifiers.

1 http://www.epinions.com/.
2 http://www.trustlet.org/wiki/Extended_Epinions_dataset.
3 http://snap.stanford.edu/data/wiki-Elec.html.
4 http://www.ehu.es/ccwintco/index.php/GIC-experimental-databases
5 http://www.cs.waikato.ac.nz/ml/weka/.
6 http://www.sands-project.eu/.

Classifier	Wikipedia			Epinions		
	OA	F1	AUC	OA	F1	AUC
NB	100	98.3	0.973	100	98.7	0.983
MLP	99.99	99.1	0.981	100	99.2	0.991
RBFC	100	98.7	0.965	100	99.3	0.971
RBFN	99.99	98.6	0.966	100	99.4	0.976
AdaBoost	100	99.4	0.986	100	99.7	0.989
JRip	99.99	98.4	0.977	100	98.8	0.975
J48	99.99	98.1	0.962	100	98.2	0.972

Table 6. Average performance results of cross-validation experiments with different classifiers over the probabilistic reputation features. (OA) Overall accuracy, (F1) F1 score, (AUC) area under the ROC.

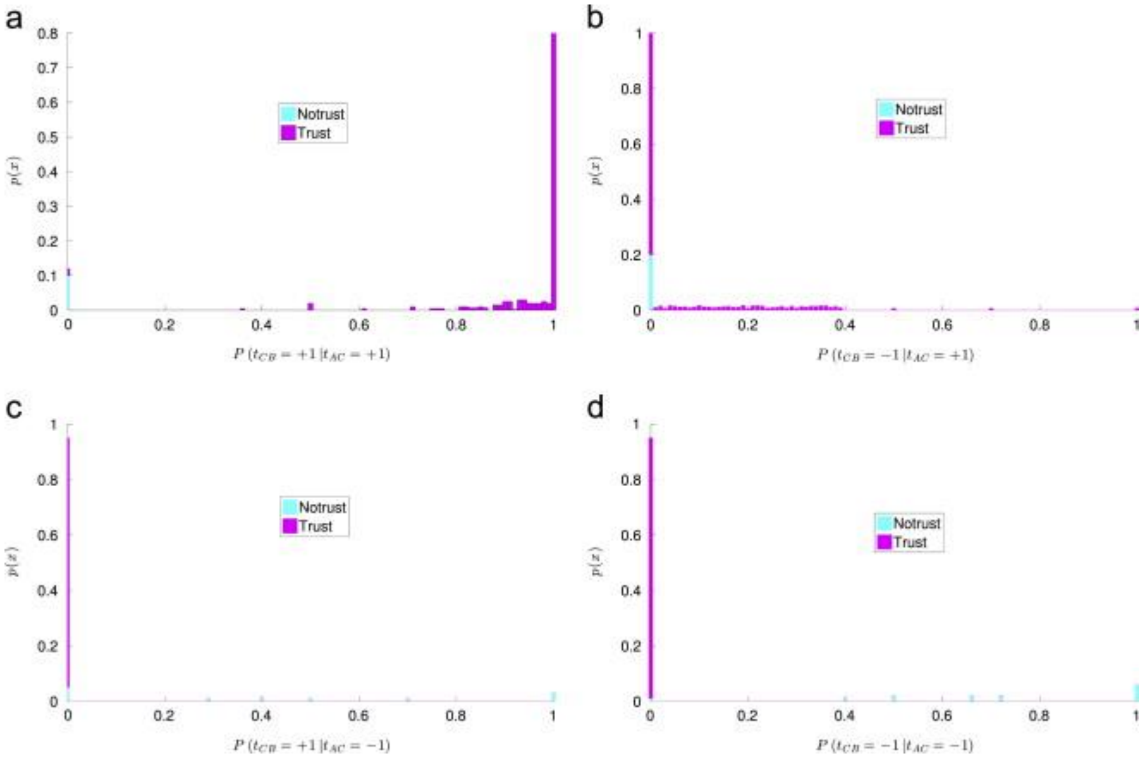

Fig. 3. *A priori* histograms of probabilistic features from Epinions database. Magenta corresponds to Trust, Blue to Notrust. (a) $P(t_{CB}=+1|t_{AC}=+1.)$, (b) $P(t_{CB}=-1|t_{AC}=+1.)$, (c) $P(t_{CB}=+1|t_{AC}=-1.)$, (d) $P(t_{CB}=-1|t_{AC}=-1.)$. (For interpretation of the references to color in this figure caption, the reader is referred to the web version of this paper.)

1 http://www.epinions.com/.
2 http://www.trustlet.org/wiki/Extended_Epinions_dataset.
3 http://snap.stanford.edu/data/wiki-Elec.html.
4 http://www.ehu.es/ccwintco/index.php/GIC-experimental-databases
5 http://www.cs.waikato.ac.nz/ml/weka/.
6 http://www.sands-project.eu/.

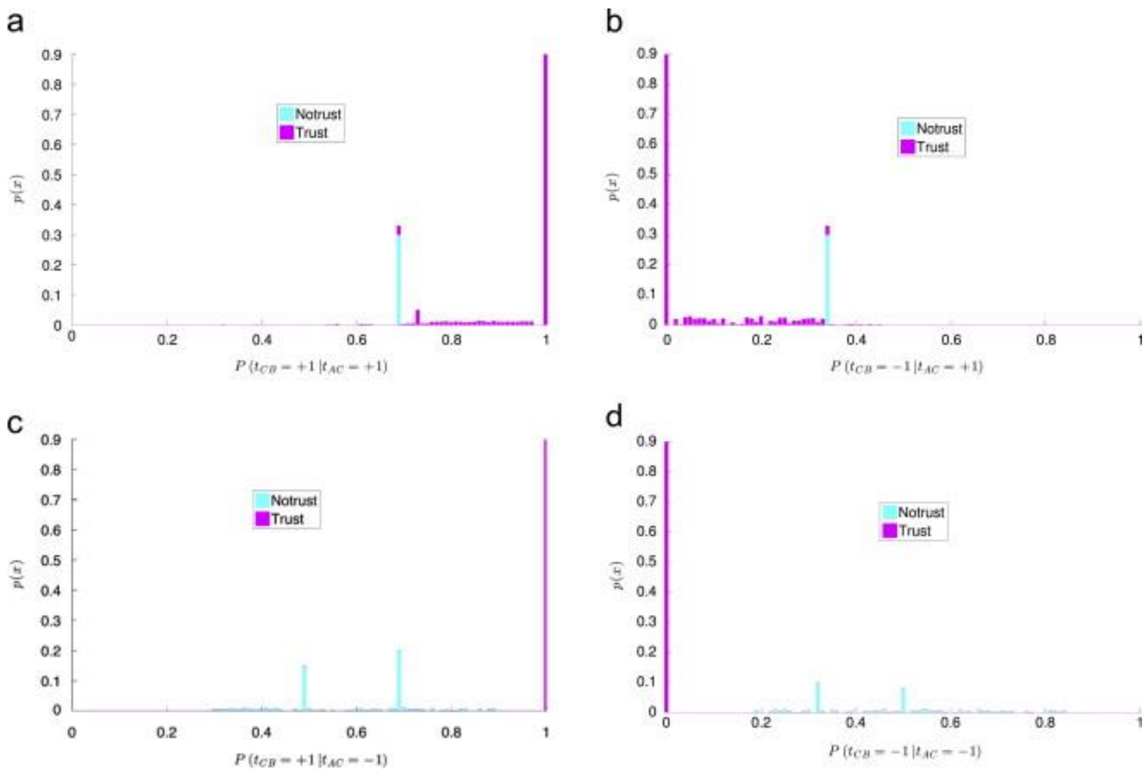

Fig. 4. *A priori* histograms of probabilistic features from Wikipedia database. Magenta corresponds to Trust, Blue to Notrust. (a) $P(t_{CB} =+ 1|t_{AC} =+ 1.)$, (b) $P(t_{CB} = -1|t_{AC} =+ 1.)$, (c) $P(t_{CB} =+ 1|t_{AC} = -1.)$, (d) $P(t_{CB} = -1|t_{AC} = -1.)$. (For interpretation of the references to color in this figure caption, the reader is referred to the web version of this paper.)

The final experiment with the probabilistic reputation features is aimed to test the ability of the classifier to stand in face of the expected continuous increase in size of the social network. To that end, we train the classifiers with a small training set and test them over the remaining database. The smaller the training set, the earlier the life of the social network. We repeat the training and testing 10 times to obtain average values. Fig. 5 shows the plot of the average accuracy obtained over the Epinions and Wikipedia reputation features. The percentages of training data go from 1% up to 99%. With the Epinions database, all classifiers achieve an accuracy of 100% from the smaller training set 1%. However, with Wikipedia we find the following:

- • AdaBoost gets an accuracy of 100% for all training set sizes.
- • NaiveBayes gets an accuracy of 99.2387% with a training size of 1%. Increasing training data size until 38% of the database, the accuracy is improved up to 99.2665%. With training sizes greater than 39% the accuracy reaches 100% (Fig. 5(b)).
- • The remaining classifiers reach an accuracy of 99.99% from a training data of 1% until 58% with little improvement. For training sizes above 59% the accuracy is 100% (Fig. 5(a)).

1 http://www.epinions.com/.
2 http://www.trustlet.org/wiki/Extended_Epinions_dataset.
3 http://snap.stanford.edu/data/wiki-Elec.html.
4 http://www.ehu.es/ccwintco/index.php/GIC-experimental-databases
5 http://www.cs.waikato.ac.nz/ml/weka/.
6 http://www.sands-project.eu/.

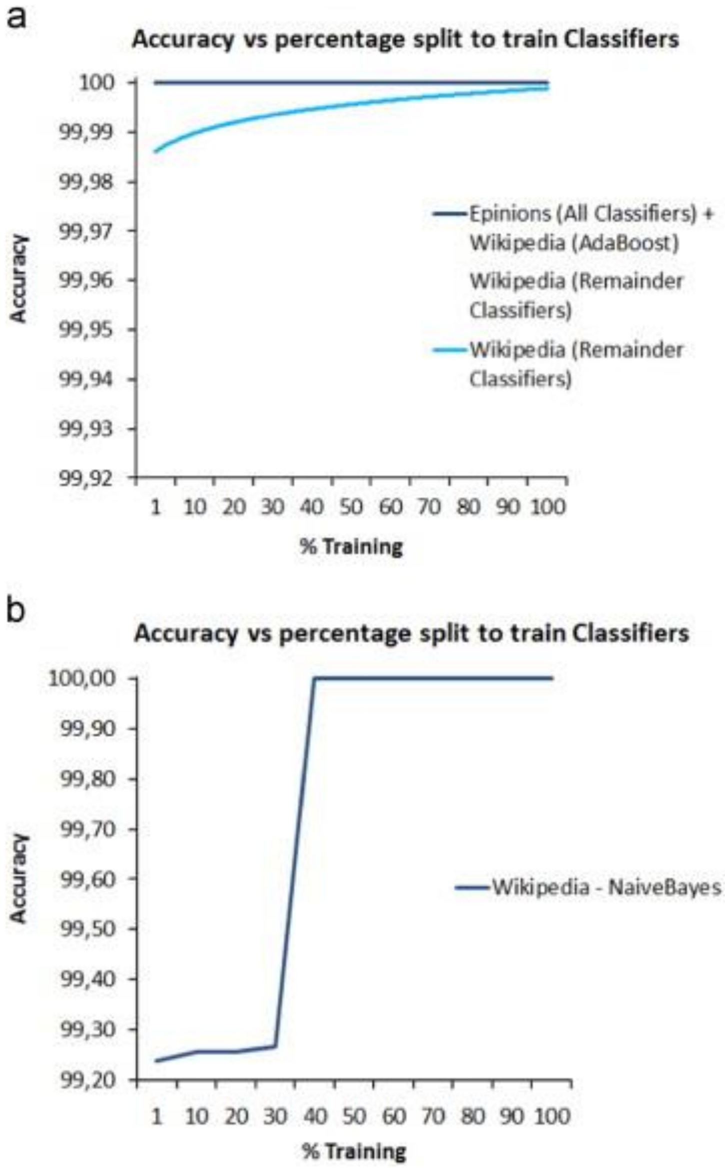

Fig. 5. Average accuracy obtained with training sets of increasing size expressed as percentage of the total database to train classifiers. (a) Joint plot of most classifiers on Epinions and Wikipedia databases. (b) Specific plot of Naïve Bayes results over the Wikipedia database.

4. Conclusions and future work

This paper introduces a Trust prediction system based on reputation features obtained from the trust values assigned by witness truster users to the trustee. The system has been demonstrated over two benchmark trust databases in the public domain, extracted from the Epinions and Wikipedia sites, respectively. We tested two kinds of features, raw reputation vectors and probabilistic reputation features. The former features lead to classification systems that are heavily influenced by the database imbalance. Attempts to improve results applying a SMOTE approach do not improve the overall accuracy, but provide improvements on the prediction of the minority class, the Notrust class. The probabilistic reputation features provide excellent results reaching 100% in both

1 http://www.epinions.com/.
2 http://www.trustlet.org/wiki/Extended_Epinions_dataset.
3 http://snap.stanford.edu/data/wiki-Elec.html.
4 http://www.ehu.es/ccwintco/index.php/GIC-experimental-databases
5 http://www.cs.waikato.ac.nz/ml/weka/.
6 http://www.sands-project.eu/.

databases. The major inconvenient is that their coverage of the Wikipedia database is small due to the existence of many singularities in the computation of the probabilities. The resiliency of the classifiers based on the probabilistic features to social network growth has been assessed by performing training experiments with very small training datasets, achieving optimal results even then.

Future work will be carried out within the framework of the SandS European project,[6] where the authors are working towards the development of a social network of home appliance users (named Eahoukers in the project) [13]. The goal is that the Eahoukers benefit from the socially generated knowledge to deal with the home appliances in a domestic environment. Trust prediction is relevant for SandS in three ways: (a) for the identification of rogue users that may try to sabotage competitors' appliances, (b) to assess the quality of the recommendations coming from specific users, and (c) to build the consensus between users. The Trust prediction system presented in this paper will be useful to assess the recommendations from other users in the elaboration of appliance use recipes. The final system will be a recommendation system enhanced by Trust prediction.

Acknowledgments

Work funded by grant agreement 317947 EU, SandS project. The author MG belongs to the UFI11/07 of the UPV/EHU.

References

1.- Kimberly S. Adams, Sandra L. Christenson Trust and the family 'school relationship examination of parents' teacher differences in elementary and secondary grades J. Sch. Psychol., 38 (5) (2000), pp. 477-497

2.- W.J. Adams, G.C. Hadjichristofi, IV, N.J. Davis, Calculating a node's reputation in a mobile ad hoc network, in: 24th IEEE International Performance, Computing, and Communications Conference, 2005, IPCCC 2005, April 2005, pp. 303–307.

3.- Donovan Artz, Yolanda Gil A survey of trust in computer science and the semantic web Web Semant.: Sci. Serv. Agents World Wide Web, 5 (2) (2007), pp. 58-71

4.- Kirsimarja Blomqvist The many faces of trust Scand. J. Manag., 13 (3) (1997), pp. 271-286

5.- Ben-Jye Chang, Szu-Liang Kuo Markov chain trust model for trust-value analysis and key management in distributed multicast manets IEEE Trans. Veh. Technol., 58 (May (4)) (2009), pp. 1846-1863

6.- N.V. Chawla, K.W. Bowyer, L.O. Hall, W.P. Kegelmeyer Smote: synthetic minority over-sampling technique J. Artif. Intell. Res., 16 (2002), pp. 321-357

7.- Jin-Hee Cho, A. Swami, Ing-Ray Chen A survey on trust management for mobile ad hoc networks IEEE Commun. Surv. Tutor., 13 (quarter (4)) (2011), pp. 562-583

8.-K.S. Cook (Ed.), Trust in Society, vol. 2, Russell Sage Foundation Series on Trust, New York, February 2003.

1 http://www.epinions.com/.
2 http://www.trustlet.org/wiki/Extended_Epinions_dataset.
3 http://snap.stanford.edu/data/wiki-Elec.html.
4 http://www.ehu.es/ccwintco/index.php/GIC-experimental-databases
5 http://www.cs.waikato.ac.nz/ml/weka/.
6 http://www.sands-project.eu/.

9.- O. Fachrunnisa, F.K. Hussain A methodology for maintaining trust in industrial digital ecosystems IEEE Trans. Ind. Electron., 60 (March (3)) (2013), pp. 1042-1058

10.- Xinmao Gai, Yong Li, Yasha Chen, Changxiang Shen, Formal definitions for trust in trusted computing, in: 2010 Seventh International Conference on Ubiquitous Intelligence Computing and 7th International Conference on Autonomic Trusted Computing (UIC/ATC), October 2010, pp. 305–310.

11.- Jennifer Golbeck, Computing with trust: Definition, properties, and algorithms, in: Securecomm and Workshops, 2006, August 28–September 1, 2006, pp. 1–7.

12.- M. Graña, J.D. Nuñez-Gonzalez, L. Ozaeta, A. Kaminska-Chuchmala, Experiments of trust prediction in social networks by artificial neural networks, Cybern. Syst. (2015), in press.

13.- Manuel Graña, J. David Nuñez-Gonzalez, Bruno Apolloni A discussion on trust requirements for a social network of eahoukers Hybrid Artificial Intelligent Systems, Springer, Heidelberg (2013), pp. 540-547

14.- Daojing He, Chun Chen, S. Chan, Jiajun Bu, A.V. Vasilakos A distributed trust evaluation model and its application scenarios for medical sensor networks IEEE Trans. Inf. Technol. Biomed., 16 (November (6)) (2012), pp. 1164-1175

15.- Lance J. Hoffman, Kim Lawson-Jenkins, Jeremy Blum Trust beyond security: an expanded trust model Commun. ACM, 49 (July (7)) (2006), pp. 94-101

16.- Jure Leskovec, Daniel Huttenlocher, Jon Kleinberg, Predicting positive and negative links in online social networks, in: Proceedings of the 19th International Conference on World Wide Web WWW '10, ACM, New York, NY, USA, 2010, pp. 641–650.

17.- Jure Leskovec, Daniel Huttenlocher, Jon Kleinberg, Signed networks in social media, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems CHI '10, ACM, New York, NY, USA, 2010, pp. 1361–1370.

18.- D.W. Manchala E-commerce trust metrics and models IEEE Internet Comput., 4 (March/April (2)) (2000), pp. 36-44

19.- P. Massa, P. Avesani, Controversial users demand local trust metrics: an experimental study on epinions.com community, in: Proceedings of the National Conference on Artificial Intelligence, vol. 1, 2005, pp. 121–126.

20.- P. Massa, P. Avesani Trust metrics on controversial users: balancing between tyranny of the majority and echo chambers Int. J. Semant. Web Inf. Syst., 3 (1) (2007), pp. 39-64

21.- Yan Lindsay Sun, Wei Yu, Zhu Han, K.J.R. Liu Information theoretic framework of trust modeling and evaluation for ad hoc networks IEEE J. Sel. Areas Commun., 24 (February (2)) (2006), pp. 305-317

22.- Daoxi Xiu, Zhaoyu Liu A formal definition for trust in distributed systems Jianying Zhou, Javier Lopez, Robert H. Deng, Feng Bao (Eds.), Information Security Lecture Notes in Computer Science, vol. 3650, Springer, Berlin, Heidelberg (2005), pp. 482-489

[1] http://www.epinions.com/.
[2] http://www.trustlet.org/wiki/Extended_Epinions_dataset.
[3] http://snap.stanford.edu/data/wiki-Elec.html.
[4] http://www.ehu.es/ccwintco/index.php/GIC-experimental-databases
[5] http://www.cs.waikato.ac.nz/ml/weka/.
[6] http://www.sands-project.eu/.