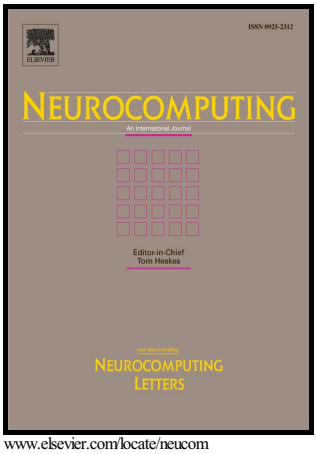

www.elsevier.com/locate/neucom

An Enhanced Trust prediction strategy for Online Social Networks using Probabilistic Reputation features

Ebin Deni Raj, L.D. Dhinesh Babu

PII: S0925-2312(16)31064-5
DOI: http://dx.doi.org/10.1016/j.neucom.2016.09.036
Reference: NEUCOM17565

To appear in: *Neurocomputing*

Received date: 27 November 2015
Revised date: 1 August 2016
Accepted date: 19 September 2016

Cite this article as: Ebin Deni Raj and L.D. Dhinesh Babu, An Enhanced Trus prediction strategy for Online Social Networks using Probabilistic Reputatio features, *Neurocomputing,* http://dx.doi.org/10.1016/j.neucom.2016.09.036

An Enhanced Trust prediction strategy for Online Social Networks using Probabilistic Reputation features.

Ebin Deni Raj, L.D. Dhinesh Babu*.

School of Information Technology and Engineering, VIT University, India

ABSTRACT

Online Social networks have gained much prominence in the recent years such that it has become an unavoidable means of daily communication. The element of trust in social networks has been studied ever since the inception of online social networks. Trust in online social networks is extremely fragile in nature due to the virtual connections between users in the network. The level of trustworthiness of each user in a social network varies and is usually computed using reputation level of the users. This paper focuses on identifying the features that determine the trust of a user in online social networks using benchmark datasets. We propose a new probabilistic reputation feature model that is better than the raw reputation features. The enhanced trust prediction framework has been tested and validated on three benchmark datasets namely *Wikipedia election* dataset, *Epinions* dataset and *Slashdot* dataset. The proposed probabilistic feature enhances the overall accuracy, F1 score, and area under the ROC for the classifier results significantly. The results have been compared with other state of the art techniques and are found to be efficient.

Keywords: Online Social Networks, Reputation features, Probabilistic reputation features, Trust Prediction, Social network analysis, Big Data.

1. Introduction

Online Social Networks (OSN) is growing every day in millions and already a third of the world population is using social networking sites like Facebook, Twitter, and LinkedIn. OSNs allow users to interact and share with other social beings and have proliferated into the daily lives of majority of the educated individuals . Mobile devices and mobile internet has accelerated the growth of OSNs to the present level. Along with the growth of OSNs, threats and attacks to gain access to personal information have also increased. OSNs have become major source for malicious attacks by employing social engineering techniques.The growth of data in OSNs has become exponential and requires more computational overhead.

Relationships in OSNs can be either positive (indicating relations such as friendship) or negative (indicating relations such as opposition or antagonism). Online interactions between users without prior real-world relationships have become common in OSNs. These kinds of interactions are based on the online reputation of the user. Even if a user is not interacting with an unknown user, he/she might get invitations/requests from friends of a known friend. The friends of a friend are indirectly connected to the user . Establishing trust among the indirectly connected users (friends of friend) plays an important role in improving the quality of social network services and enforcing security of the users. In OSNs trust is built from experience along a feedback process . Trust in OSNs is researched and organized into four major topics (1) Policy based trust; (2) Reputation based trust (3) General models of trust and (4) Trust information resources . Most of the research in trust prediction aims in proposing a trust framework to address and predict trust. The objective of trust prediction in OSNs is to address the issue, "Can Alice trust Bob to add him to her network of friends?" The trust prediction even helps in assessing threats to country, region or race.

Reputation and trust prediction are considered as "soft security" mechanisms which help assessing another user without knowing the user. There are various trust prediction systems for online social networks as well as for e-commerce networks. Most of the trust prediction systems suffer from cold start problem. Cold start problem is an issue in recommendation systems and online social networks where the prediction framework cannot provide effective suggestions to the users as it does not have enough annotated information . Both, optimal solutions as well as the approximation solution to cold start problem are NP hard. Trust prediction becomes more relevant when a new user joins the network and the credibility of the user has to be judged. The prediction has to be done in a scenario in which there is no previous experience available on the trustee behaviour.

The prediction of trustee behaviour from indirect information like reputation information from third party witnesses has high relevance during cold start problem. Trust prediction is usually treated as a classification problem. Reputation is treated as the best guess information which can be used to predict the trust worthiness of a trustee . Even though the relation between