SoundMeGood: A Trust Model Supporting Preliminary Trust Establishment Between Mutually Unknown Entities

Roman Špánek, Pavel Tyl

***Abstract*—**The paper proposes a SoundMeGood trust model being able to establish a preliminary trust level among unknown users in a distributed environment. Computation of preliminary level of trust is based on similarities among users based on various components of their profiles. As a metric used for similarity computation has been used and experimentally evaluated DTW* algorithm.

***Keywords*—**Trust, Social Network, Trust Management System, Distributed Systems.

I. Introduction

SOCIAL Networks (SNS) has been very popular for quite a sometime and currently they seem to be given even more popularity and companies providing these systems are becoming even more successful. Such tremendous success can be easily understood as the communication has been the main factor influencing the human society evolution since time immemorial. Therefore almost all communication technologies and communication medias (especially the Internet) has been predestined to success.

In the paper we propose a novel trust model that enables trust establishment in situations where there is no or very limited amount of former information (a transaction history) or when users cannot meet directly (personally). Such situations occur for instance in an audience of participants of a conference where each and every participant has only one direct way how to find out which topics other participants are interested in and therefore who might be a good partner for discussion or common work. Other scenarios include situations where business partners try to establish a new partnership or identify common business interests.

II. Related Work

The importance of trust is indisputable in majority of contemporary communication or eBussiness platforms. Most of the trust management systems are designed to build trust between entities based on their *transaction history*. A transaction is the central point giving majority of input data a reputation system is transferring to a scale representing trust (note that trust and reputation are very close terms and there exists a straightforward transition from trust to reputation). A trust scale can be of many different types, for example (from 0 to 5 stars; a binary positive/negative; a choice from a scale ranging from poor to excellent; a natural number from 1 to 10).

Several trust management systems have been proposed to maintain security in open and distributed systems, service-oriented environments [3], Semantic Grids [7] and multi-agent societies [6].

Some trust management systems use centralized approach where a dedicated centralized unit is responsible for maintaining trust between entities. Such approaches may be thought of as a more reliable since centralized unit has generally greater security controls, but it also presents a single point of failure. Thus, fully or partially distributed trust management systems have been proposed to overcome the disadvantages of centralized unit architecture.

Other approaches try to define a different notion of formulation. For example let us mention fuzzy logic [1] or game theory models [5]. Different formulation model may be more appropriate within a different target environment or may provide better flexibility in a particular system.

Some other proposals are using ontologies for conceptualization of quality of service (QoS) [4].

Many systems have been designed without any standardization. In other words, trust management systems have been proposed and designed particularly for a target environment. Such situation was identified as a possible issue and several works have tried to identify common parts [2]. Such studies are very important as it is shown that despite differences in for example computational models, the following main building blocks can be found in all or at least majority of trust management systems:

- gathering behavioral information,
- computation phase; scoring and ranking entities (peers, nodes, agents, and sensors),
- entity selection,
- transaction,
- and rewarding and punishing entities.

Roman. Špánek Institute of Computer Science of the Czech Republic, Pod Vodárenskou věží 271/2, Prague, Czech Republic (phone: +420 535 35 19 ; fax: +420 535 35 19; e-mail:spanek@cs.cas.cz).

Pavel Tyl, Technical University of Liberec, Studentská 2, 46117, Liberec, Czech Republic

Currently used trust management systems usually compress components influencing final reputation into a one number (set of stars or other symbols having some semantics being clearer to users). This is usually done by mapping trust components using a particular computation model on a value representing a user trustworthiness.

A. The Dynamic Time Warping Algorithm Introduction

The Dynamic Time Warping algorithm (DTW) is a well-known algorithm in many areas. While first introduced in 60s [8] and extensively explored in 70s by application to the speech recognition it is currently used in many areas: handwriting and online signature matching, sign language recognition and gestures recognition, data mining and time series clustering (time series databases search), computer vision and computer animation, surveillance, protein sequence alignment and chemical engineering, music and signal processing.

DTW algorithm has been proposed to address an issue for searching similarities between the time-series minimizing the effects of shifting and distortion in time by allowing "elastic" transformation of time series in order to detect similar shapes with different phases. Given two time series $X = (x_1, x_2, ... x_N); N \in \mathrm{N}$ and $Y = (y_1, y_2, ... y_M); M \in \mathrm{N}$ represented by the sequences of values (or curves represented by the sequences of vertices) DTW yields optimal solution in the *O(MN)* time which could be improved further through different techniques such as multi-scaling. The only restriction placed on the data sequences is that they should be sampled at equidistant points in time (this problem can be resolved by re-sampling).

III. Challenge Description

The main challenge is to have a system that enables a preliminary trust establishment between users within a limited time, by sharing minimum personal information (name, affiliation etc.) and by usage of limited resources.

Since trust has been managed by many different reputation systems, a direct comparison of trust and its transition from a one system to another one is also a challenge.

In this paper we present basic building blocks of the trust management system being currently designed by our team at Technical university of Liberec and Institute of Computer Sciences Academy of Sciences of the Czech Republic. Particularly, in the following we present:

- The SoundMeGood trust model;
- The SoundMeGood metric used for computing preliminary trust level between users.

IV. The SoundMeGood Trust Model

Note, that proposals and results in this paper concern only two building blocks of the SoundMeGood[1] system, which are currently under implementation.

A. A SoundMeGood Model Requirements

The following requirements seem to be fundamental for a trust management system providing required functionality from our point of view:

- Simplicity - preliminary level of trust has to be given straightforwardly in a simple and user friendly format;
- Extensibility - a model extension has to be done by simple, transparent and straightforward way;
- Implementability - implementation of a model has to be achievable even on devices with limited resources.

B. The SoundMeGood Trust Model Proposal

The important fact influencing creation and management of trust is to preserve as much as possible about a user peculiarities. Thus, in the following items have been identified as all available inputs for the SoundMeGood model:

- level of trust build in another system (if there is a transaction history available, it ought to be also included);
- a user profile (basic information about a user);
- a user preferences (what she likes and dislikes).

We will call these inputs as *trust components* in the rest of the paper.

The SoundMeGood model takes all available inputs - trust components - and maps these onto a two dimensional space with trust components on the x-axe and values given for each of the trust components on the y-axe (see section IV.C for details on x (section) and section IV.D for details on y axes mappings).

The trust components can be seen as a sequence $C = (c_1, c_2, ... c_N); N \in \mathrm{N}$. We will call this sequence the *trust sequence*. A graphical depiction of trust components will be called the *trust function* and it is created as a simple spline connection of adjacent trust sequence components.
Given two different users, the task is to find how similar these trust sequences are. Evaluation of similarities is the main task for the SoundMeGood metric (see section VI for details).

C. An x-axe Mapping Proposal

Mapping of a user profiles onto x-axe is important as the SoundMeGood metric is sensitive to the x-axe ordering and scaling. The SoundMeGood ontology (see section V) is used to map each trust component of a user profile to a trust sequence. Created trust sequence is simply mapped to the x-axe using predefined sampling frequency (sampling frequency might be different in different cases, but has to be same for both users' profiles being compared by the SoundMeGood metric).

D. An y-axe Mapping Proposal

One of the main advantages of the SounfMeGood model is its insensitivity to concrete trust component values. Therefore mapping trust values to the y-axe is simple. For the sake of generality we propose to have reals on the y-axe as most values can be mapped to reals, but SoudMeGood metric is not sensitive to this.

[1] The name suggests a basic idea that is grounded on a different sensitivity of users to a various music genres.

V. THE SOUNDMEGOOD ONTOLOGY

The SoundMeGood metric is sensitive to ordering of the trust sequence components. To provide the same ordering we propose to use an ontology describing basic widely accepted trust components (we omit details on the ontology in this paper for given space constraints).

The main task of the ontology is to map each trust component to a particular trust sequence component preserving trust sequence ordering. The usage of the ontology also enables its further extension by extending the ontology or by matching/joining with other existing ontologies.

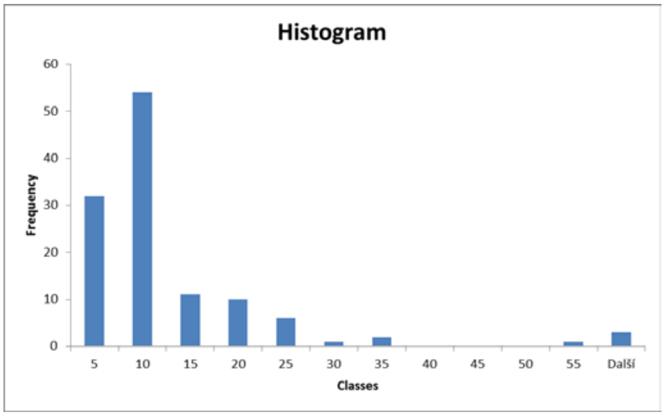

Fig. 3 Histogram representing distribution of distances evaluated by DTW*

VI. THE SOUNDMEGOOD METRIC

The SoundMeGood metric has to be able to find similarities between trust sequences and since trust sequences might have different values of each trust component, it has to be insensitive to this.

We believe that important are not particular values of trust components but rather a profile/shape of the trust function in general. We have selected DTW (see section II) algorithm to be the basic for the SoundMeGood metric. Since we are proposing some modifications (results in the paper presents experiments run with non-modified one) to the DTW we will call the SoundMeGood modification as DTW*.

DTW* provides similarities between two trust sequences given as an input and produces a real number expressing similarity as its output. It is important to have just one number expressing the similarity as it immediately shows the results to a user in a comprehensible form, but note that this number corresponds to the shape of the trust function, to each and every trust component.

VII. EXPERIMENTS

A first set of experiments that have been set up at the Technical University at Liberec has focused the evaluation of ability of the SoundMeGood model to establish preliminary level of trust between unknown users. Students and academic stuff at the university were asked to fill a simple questionnaire containing just 18 questions all organized into 3 groups (music, movies and sports). Each respondent fills her preferences on a scale from 0 to 10.

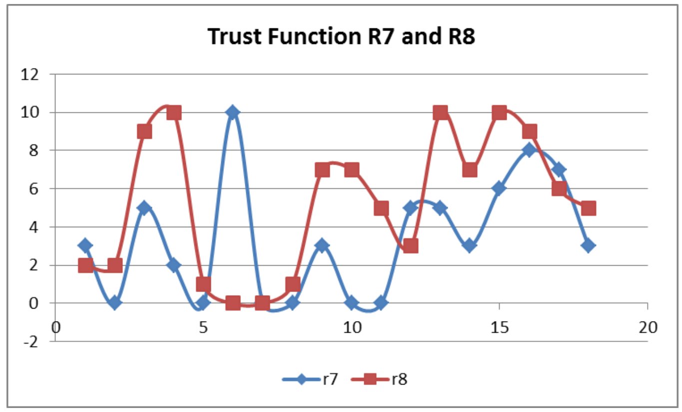

Fig. 1 Trust functions with the best DTW* match

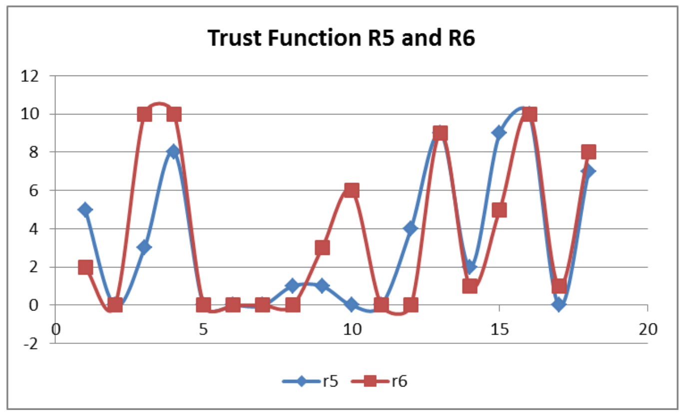

Fig. 2 Trust functions with the best AVG match

In Fig. 3 a histogram of distances evaluated by DTW* algorithm between trust sequences of the respondents is presented. It is important to know the distribution of distances and to verify that there is a threshold separating respondents being close to themselves and those that are too distinct. From the histogram it is clear that such threshold can be found between DTW* distances 10 and 15. Moreover, detailed evaluation has shown that distance bellow 7 can be seen as very good match. For experiments and comparison we have also implemented a second simple measure evaluating respondents' similarity. The second measure is a sum of absolute values of differences between respondents replies (will be called AbsolutValue Distance - AVD in the rest).

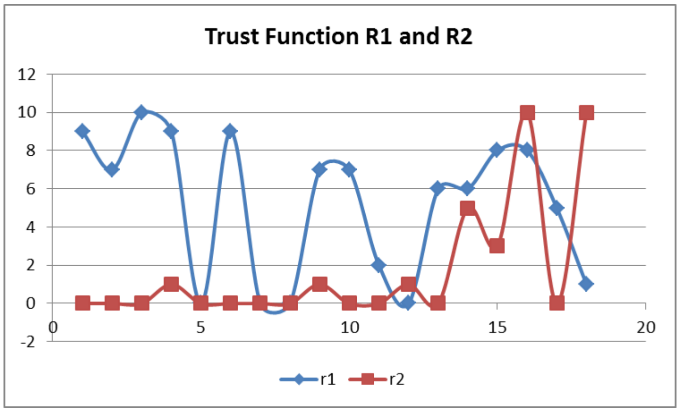

Fig. 4 Trust functions with the worst DTW* match

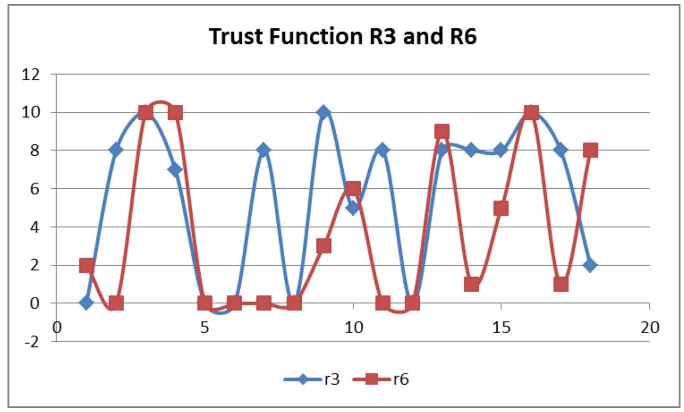

Fig. 6 Trust functions of profiles with a little AVD match but a good DTW* match

Fig. 1 shows trust function of two respondents that have the best match (DTW* distance 2.321) and in figure Fig. 2 two respondents being evaluated as the best match by AVD (note that DWT* distance of this case is 3, which is also one of the best).

Fig. 4 and Fig. 5 show the same but for the worst matches by DTW* and AVD, respectively.

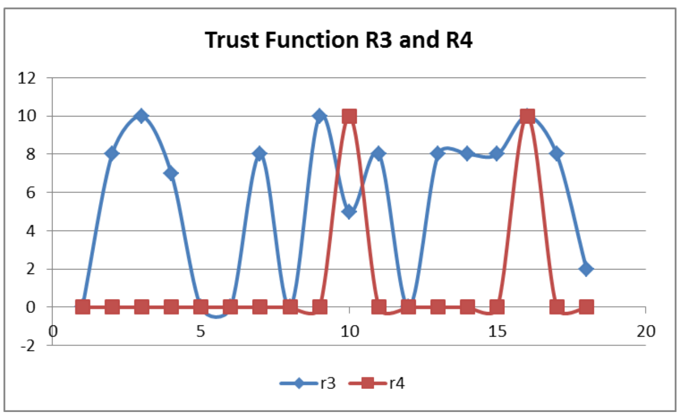

Fig. 5 Trust functions with the worst AVD match

In the last figure Fig. 6 an interesting situation is depicted. The depicted trust sequences were evaluated as quite a good match by DTW* (DTW* distance is 3.538) but they have been evaluated as to different by classical AVD. From the figure it is quite clear that these trust sequences are quite close (the worst match is in the middle, which corresponds to the music group of questions), but the rest is in very good match. From that case it is clear that DTW* performs better than AVD, but more importantly it was able to revel similarity of respondents.

VIII. Conclusion and Future Work

The paper presents a model that enables evaluation of a preliminary level of trust between users based on the similarity between their trust components. Similarity evaluation is given by DTW* algorithm, which is able to find similarity between two trust sequences. The experiments have shown that such approach can be a good first approximation.

The SoundMeGood model has also ability to find similarities in profiles from different social networks (systems) where no mapping of trust component values to a common scale is needed and such profiles can be compared directly.

The future work will aimed more precise evaluation of DTW* under a different scenarios and to proposal of a DTW* modification that will be more sensitive to a situation where one of trust components of two respondents is very different.

The preliminary experiments have also shown that using DTW* on a parts of the whole profile and its further processing (even by a simple DTW again) can provide more precise results.

There exists also a simple implementation of SoundMeGood for mobile devices (equipped with J2ME and BlueTooth communication technologies), which will be used for an experiment with in a Technical University campus.

Acknowledgement

The work was supported by the project GAP202/10/0761 Web Semantization" and by the student grant SGS 2011/7821 Interactive Mechatronics Systems Using the Cybernetics Principles".

References

[1] Kamal Bharadwaj, Mohammad a. h. y. a. Al-Shamri: *Fuzzy computational models for trust and reputation systems*. Electronic Commerce Research and Applications, Vol. 8, No. 1. (January 2009), pp. 37{47. DOI: 10.1016/j.elerap.2008.08.001.

[2] Loubna Mekouar, Youssef Iraqi, Raouf Boutaba: *Reputation-Based Trust Management in Peer-to-Peer Systems: Taxonomy and Anatomy*. Handbook of Peer-to-Peer Networking, , Volume . ISBN 978-0-387-09750-3. Springer Science+Business Media, LLC, 2010, p. 689

[3] Zaki Malik, Athman Bouguettaya: RATEWeb: *Reputation Assessment for Trust Establishment among Web services*. The VLDB Journal, Vol. 18, No. 4. (2009), pp. 885{911.

[4] E. Michael Maximilien, Munindar P. Singh: *Agent-based trust model involving multiple qualities.* Proceedings of the 4th International Joint Conference on Autonomous Agents and Multiagent Systems, July 25 - 29, 2005, The Netherlands.

[5] Ruggero Morselli, Jonathan Katz, BobbyBhattacharjee: *A Game-Theoretic Framework for Analyzing Trust-Inference Protocols*. Proceedings of the 2nd Workshop on the Economics of Peer-to-peer Systems, 2004.

[6] Jordi Sabater, Carles Sierra: *Reputation and social network analysis in multi-agent systems*. Proceedings of the 1st International Joint Conference on Autonomous Agents and Multiagent Systems: Part 1, July 15{19, 2002, Bologna, Italy.

[7] Florian Skopik, DanielSchall,Schahram Dustdar: *Modeling and mining of dynamic trust in complex service-oriented systems*. Distributed Systems Group,Vienna University of Technology,Argentinierstr 8/184-1,1040 Vienna, Austria, 2010.

[8] Pavel Senin: *Dynamic Time Warping Algorithm Review*, Technical Report - University of Hawaii at Manoa, 2008.