Towards Intuitionistic Fuzzy Relational Webs of Trust and Distrust

Martine De Cock
Ghent University
Dept. of Appl. Math. and CS
Krijgslaan 281 (S9)
9000 Gent, Belgium
Martine.DeCock@UGent.be
http://www.fuzzy.UGent.be

Paulo Pinheiro da Silva
Stanford University
Knowledge Systems
AI Laboratory
Stanford CA 94305, USA
pp@ksl.stanford.edu
http://iw.stanford.edu

The interest in trust computing is growing significantly [1]. Mechanisms based on the human notion of trust can not only contribute to, but seem even vital for the effective use of web applications accessing multiple information sources. For example, question answering engines are useful only to the degree to which the user trusts the sources that are used in deriving the answer. As the amount of available information sources increases, so does the challenge in trusting or sometimes distrusting them. The advice offered by a recommender system is taking into account only to the extent to which the recommenders are trusted.

In a large system, it is unlikely for a single agent to know all sources or all recommenders well enough to express a level of trust in them. In a more realistic setting, an agent expresses trust only in a few other agents. They, in turn, also express their trust, and as a result a web of agents arises. Even when there is no direct connection between agents a and b, agent a can still attempt to compute trust information about b by consulting trusted third parties. This is called trust propagation.

Existing computational models usually deal with trust in a binary way: they assume that an agent is to be trusted or not, and they compute the probability or the belief that the agent can be trusted. Besides full trust or no trust at all, in reality we also encounter partial trust. This is reflected in our everyday language when we say for example "this source is rather trustworthy" or "I trust this source very much".

Hence we propose the possibility to deal with trust as a matter of degree. This is particularly useful in situations where agents can not be divided in

the trustworthy ones and the malicious ones in a clear cut way, but they can be trusted to a certain extent. Whereas the existing probabilistic approach is suitable for problems where security is at stake and malicious sources need to be discerned from trustworthy ones, our approach leans itself for the computation of trust when the outcome of an action can be positive to some extent, e.g., when provided information can be right to some degree, as opposed to being either right or wrong. We use a number t between 0 and 1 to express the degree of trust of a in b. This value is neither a probability nor a belief. In a probabilistic setting, a higher trust level corresponds to a higher probability that an agent can be trusted, while in our interpretation it corresponds to a higher trust. Both approaches are complementary.

Furthermore, in our model, 0 corresponds to total absence of trust. Roughly speaking, this can occur in either one of the following situations: (1) a has reason to distrust b fully, or (2) a has no information about b and hence no reason to trust b, but also no reason to distrust b. Taking into account the fundamental difference between the two situations, and the fact that distrust is no less important than trust in relying on an information source or a recommender, we propose to represent distrust d simultaneously with trust as a couple (t, d), in which both t and d are numbers between 0 and 1. Trust and distrust do not have to sum up to 1, but we assume that they satisfy the restriction $t + d \leq 1$. As a result, the web of trust between agents is represented by an intuitionistic fuzzy relation. Omitting the restriction $t + d \leq 1$ results in allowing inconsistency — an interesting option for future development.

The problem of atomic trust propagation can informally be described as: if the trust value of source a in source b is p, and the trust value of b in source c is q, what information can be derived about the trust value of a in c? This problem has been well researched in a probabilistic setting, where multiplication is used as the main operation to combine trust values. However, when distrust is involved as well, the need for a new, not necessarily commutative propagation operator arises.

References

[1] P. Herrmann, V. Issarny, S. Shiu, **Trust Management**, Third International Conference, iTrust 2005, Lecture Notes in Computer Science 3477, (2005)