January 2010

# Trust and Reputation Systems: Research Topics

*The Internet has enabled the creation of virtual worlds and communities, where user interaction imitate and, to some extent, even replace the more traditional “real-life” equivalents on a larger scale. The existence of easily accessible virtual communities makes it both possible and legitimate to communicate with total strangers.*

*Trust and reputation systems are considered key enablers of virtual communities, especially communities of strangers, where users are not required to reveal their real identities and use nick-names or pseudonyms instead. These systems support the accumulation of member reputation information and leverage this information to increase the likelihood of successful member interactions and to better protect the community from fraudulent members.*

# Research Topics

## Trust Metric

Trust and reputation are obtained from the information provided by members of the community about interactions they had with other members i.e. rating information. One of the main goals of researches on trust and reputation systems is to determine a suitable computerized representation of trust and design the algorithms for reputation computation.

The challenge is to have a trust metric that is both intuitive and theoretically convincing. One direction in this respect is to use belief theory. The Dempster- Shafer belief theory is very useful when it is important to make a decision based on the amount of evidence that has been collected, as in the case of ratings. Related to this theory, Josang's subjective logic is suitable for modeling and analyzing situations characterized by uncertainty and incomplete knowledge such as trust networks. Since we have done previous work on a deterministic model for computing reputation, one direction of research may be extension of this model with uncertainty and belief theory.

## Community Clustering Algorithm

A partition of the community to subsets of community members identified as having overall strong trust relations among themselves, allows one to utilize information from members she trusts. Every member should trust any other member in her group of trust above some threshold.

The problem of identifying groups of trust (knots) in a trust network is modeled as a graph clustering problem, where vertices correspond to individual items and edges describe relationships. Under this interpretation, a community is represented by a directed graph, in which vertices represent members and edges represent the trust relations between the members represented by their end-point vertices.

A path between two vertices that are not connected by an edge represents the transitive property of trust (e.g. Alice trusts Bob + Bob trusts Clair => Alice trusts Clair).

Correlation clustering is a powerful technique for discovering groups of trust in graphs. It operates on the pair-wise relationships between vertices, partitioning the graph to maximize the number of related pairs that are clustered together, plus the number of unrelated pairs that are separated. We investigate heuristic algorithms for correlation clustering with restricted clusters diameter size (to avoid trust based on long paths of transitive trust). Future work will suggest additional heuristics and try to estimate the tradeoff of optimality/performance.

## Update Policy

The community network is a dynamic data structure. Trust and reputation are adjusted constantly as a result of experience gained in community activities. We seek for the best way to update clusters (groups of trust, knots) based on the activities performed within the community. On the one hand we would like to quickly identify members that should be excluded from their knot (potential malicious members) and on the other hand we want to avoid frequently moving members in and out a knot. We also like to give the most accurate reputation estimation without burdening the system with too frequent updates. Different policies for updating knots should be considered, such as regularly (daily) or upon a predefined number of clustering constraints violations.

## Attacks

We consider common attacks on communities (e.g. self-promoting, whitewashing, slandering). Our goal is to design the means to protect the community from these attacks while allowing innocent members to make mistakes or hold a different opinion. The system should be tolerant to honest mistakes, but at the same time defend itself against malicious users. We believe that the knots model can be a good basis for initial identification of suspicious users, but additional information may be needed, possibly information of users' behavior in other communities. The CCR (cross-community reputation) model developed by us can be a useful tool in this direction. The research will attempt to identify malicious users while minimizing false positives and embarrassment to honest but non-regular users.

## Distributed Model

As part of our previous research we designed and implemented an infra-structure called TRIC – Trust and Reputation infra-structure for virtual communities. In order to support large communities with hundreds of thousands of users one need to consider a distributed architecture. In order to design a distributed version of our model we want to investigate the following issues:

• Designing a distributed storage scheme

• Efficient storage of aggregated data

• Distributed Rating and privacy-preserving rating submission

• Distributed Privacy-preserving request/response process

All of the above are suitable topics for MS theses, some may be suitable for a PhD, and some may be supported by a grant.