PhD Proposal on Reputation for Peer-to-Peer systems

Emmanuelle Anceaume, EPI Adept, anceaume@irisa.fr

1 Host Laboratory

EPI Adept, INRIA Rennes Bretagne Atlantique
Campus de beaulieu, 35042, Rennes Cedex France.

2 Thesis subject: Robust Reputation Mechanisms for P2P Systems

The Adept research group addresses both dependabilities issues (reliability, availability, and security) involving resources (computers and data) in both medium-scale and large scale dynamic systems. We focus on models, algorithms, and tools necessary to understand, build and prove distributed systems.

In recent years, digital reputation systems have emerged as a way to reduce the risk entailed in interactions among strangers involved in electronic transactions. Such systems collect and aggregate feedback about the past behaviour of participants, so as to derive reputation scores that should help in predicting future transaction behaviour. Clearly, without such mechanisms the temptation to act abusively for immediate gain can be stronger than the one of cooperating. The efficiency and accuracy of a reputation system depends on nodes willingness to participate. However there is a trade-off between collecting a sizeable amount of feedback and facing unreliable feedback. Nodes may attempt to collectively subvert the system[1] by either discrediting the reputation of a target node to lately benefit from it (bad mouthing) or by advertising the quality of service of a target node more than its real value to increase its reputation (ballot stuffing) [2]. In the worst case, reputation systems may have to face sybil attacks, that is nodes that pollute the system by creating numerous fake identifiers [3]. In addition to these attacks, nodes providing feedback would like to be sure that the opinion they provide cannot be abused by malicious nodes (collectively or not) in a way that can affect them in the future (e.g., through retaliation). Anonymous feedback should encourage truthfulness by guaranteeing secrecy and freedom[4]. Note however that this freedom might also be exploited by malicious nodes through bad mouthing or ballot stuffing.

In this context, the main objective of this PhD project is to design efficient and secure reputation that scale, in the presence of undesirable behaviors (collusions and sybil attacks). The student will focus on incentive for participation, and on mechanisms to detect and/or prevent the presence of collusions and sybil attacks, and counter hidden action attacks. The combination of privacy and complementary mechanisms promoting truthful feedback (e.g., tit-for-tat mechanisms) will be studied as they should make reputation mechanisms more robust than ever.

References

[1] E. Anceaume and A. Ravoaja. Incentive-based robust reputation mechanism for Peer-to-peer services. In Proceedings of the International conference on Principles of Distributed Systems, 2006.

[2] M. Feldman, K. Laio and J. Chuang. Robust incentive techniques fir peer-to-peer networks. In

Proceedings of the 5th ACM conference on Electronic Commerce, 2004.
[3] J. Douceur. The sybil attack. In Proceedings of the 1rst International Workshop on Peer-to-Peer Systems, 2002.
[4] Supporting privacy in Decentralized additive reputation systems, E. Pavlov, J. Rosenschein, and Z. Topol, iTrust 2004

More information can be obtained from Emmanuelle Anceaume (anceaume@irisa.fr, IRISA).