

Reputation Management for Content Distribution

abstract submitted to *Workshop on Content Distribution on December 9-10 2004*

Roberto G. Cascella

cascella@dit.unitn.it

Netmob Group (Computer Networks and Mobility)

Department of Communication and Information Technologies, Università di Trento - Italy

Peer to peer networks are being actively used to facilitate the distribution of content by avoiding the bottlenecks given by a single server [1]. However, the success of peer to peer systems depends heavily on the users' behavior: they can cooperate and distribute the content, they can act selfishly (free-riders) or, even worse, they can insert tampered content into the network. Malicious behavior decreases the number of successful transactions and therefore the efficient functioning of peer to peer systems must control the spreading and the effects of malicious users.

Battiti et al. [2] recently proposed the ROCQ scheme (Reputation, Opinion, Credibility and Quality), a reputation-based trust management system that uses opinions from past interactions to measure the trustworthiness of a peer. In particular the reputation of a node is calculated by considering the credibility of the reporting peers and the first-hand opinion of the user. ROCQ also introduces the quality of an opinion as a parameter to express the strength that a node poses on its opinion.

The ROCQ scheme used in a content distribution network can provide a measure of the quality of service a user is likely to provide. The reputation values can be used as basic measures to activate feedback mechanisms that encourage active participation and discourage malicious behavior. The simple scheme is effective when the content is downloaded from a single source, but has limitations when multiple sources upload a file. This happens because the integrity of the file can be verified only when all chunks have been downloaded and assembled. A fine-grained integrity control on each piece of a file has been implemented in BitTorrent, but here it is still possible to upload chunks of pieces from different sources.

With no integrity protection and the content divided into multiple parts, a malicious user can provide inauthentic chunks and not easily be localized. If the basic ROCQ scheme is used, the malicious node cannot be isolated from other nodes that have contributed to the entire content. Therefore, assigning a bad opinion to all nodes lowers the reputation of both the bad node and the good ones. Currently, we are investigating solutions to solve this issue and other issues arising in content distribution schemes based on the cooperation of dynamic coalitions (virtual communities) of users.

[1] E. Biersack, P. Rodriguez and P. Felber. "Performance Analysis of Peer-to-Peer Networks for File Distribution". In *Proceedings of the Fifth International Workshop on Quality of Future Internet Services (QofIS'04)*, September 2004.

[2] R. Battiti, A. Garg and G. Costanzi. "Dynamic Self-management of Autonomic Systems: The Reputation, Quality and Credibility (RQC) Scheme". In *The 1st 1 IFIP TC6 WG6.6 International Workshop on Autonomic Communication*, October 2004.