Reputation for Self-preservation of Autonomic Systems*

Roberto Cascella
Dipartimento di Informatica e Telecomunicazioni,
Università di Trento,
Via Sommarive 14, 38050 Povo (TN), Italy
cascella@dit.unitn.it

Autonomic systems aim at incorporating methods to monitor their dynamic behaviour and to react in automated ways in order to effectively reconfigure themselves to adapt to new environments. In the context of computer communication networks and distributed system, heterogeneous entities without any centralized organization or control interact to propagate information or to create new services according to the nodes' capabilities and to the network requirements, and at the same time, to respond autonomically to network changes.

This results in a new self-organized paradigm centred on the entities participating in the system. By making nodes service providers in addition to being service consumers, their responsibility increases in sustaining the utility of the system which relies entirely on the behaviour of users and on how they will contribute toward system goals.

End-user cooperation is one of the major problems in autonomic communication systems as entities try to maximize their own benefit without contributing to the system actively. These nodes, called misbehaving, can expose either a harmful behaviour, when they are controlled by malfunctioning components or malicious users that wish to disrupt the network, or simply they can be selfish when non-cooperation results in greater benefit.

In this context, reputation management systems are an invaluable tool to control the system and to monitor the user contribution to overall system goal. The concept of reputation has been already used in the past and applied in many different fields to have an estimation of the expected quality of the user or nodes in providing a service. In autonomic communication systems we can refer to reputation as the expected behaviour of a user in a service transaction.

Many reputation schemes have been proposed in literature and have been deployed for different context ranging from peer-to-peer or content distribution networks [2–5] to mobile ad-hoc networks [1, 6] with different goals and requirements in mind. The common framework consists of monitoring how nodes behave in transactions with other nodes and defining a metric to quantify their trustworthiness. As the reputation value of a node is determined based on the history, the system relies on the dissemination of trust information gathered through transactions between nodes so that past experience can be evaluated

*Work supported by the project CASCADAS (IST-027807) funded by the FET Program of the European Commission.

and generalized to predict the behaviour of the node in the future. This information is then shared among nodes who can decide whether interact with trustworthy nodes or ignore malicious nodes.

However, to sustain the dynamic nature of autonomic systems and to have a mechanism that adapts the reputation scheme to network changes, components must be continually evaluated for their cooperation and the aggregation (aging the input to determine the evolution of the trust value of the node) and the dissemination of the new computed reputation value should be immediate to reflect the current behaviour of the a node. Furthermore, autonomic communication systems are characterized by the presence of components that have also interested in short and not durable interactions. In this context, the rapid evolution of the system and possibly the lack of information on the prior node behaviour complicate the determination of its trustworthiness.

Therefore, the heuristics that define the trust value of a node should somehow consider the dynamicity of the system and the duration and importance of interactions in the computation of the aggregated reputation value, mainly in presence of limited and sparse connectivity of the nodes. Components that have sporadic transactions require the calculation of their reputation value to converge fast even if the measure is not precise and accurate. In this case, the computational time of the reputation of a node cannot be a critical factor.

On the contrary, permanent nodes in the network want to create a web of trust with complete information on the trustworthiness of other users. These nodes can interact continually, thus, the computation of their reputation value can rely on more input information and be more accurate. Currently, we are investigating solutions to solve this issue and other issues arising in autonomic communication networks based on the cooperation of dynamic coalitions (virtual communities) of users.

References

[1] S. Buchegger and J.-Y. L. Boudec. Performance analysis of the confidant protocol. In *MobiHoc '02: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, pages 226–236, Lausanne, Switzerland, 2002.

[2] A. Garg, R. Battiti, and R. Cascella. Reputation management: Experiments on the Robustness of ROCQ. In *Proc. of the 7th International Symposium on Autonomous Decentralized Systems (1st International Workshop on Autonomic Communication for Evolvable Next Generation Networks)*, pages 725–730, Apr. 2005.

[3] A. Garg and R. Cascella. Reputation management for collaborative content distribution. In *Proceedings of the First International IEEE WoWMoM Workshop on Autonomic Communications and Computing*, pages 547–552, Taormina, Italy, June 2005. IEEE Computer Society.

[4] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina. The eigentrust algorithm for reputation management in P2P networks. In *Proceedings of the 12th international conference on World Wide Web*, pages 640–651, Budapest, Hungary, 2003.

[5] S. Lee, R. Sherwood, and B. Bhattacharjee. Cooperative peer groups in NICE. In *IEEE INFOCOM 2003*, volume 2, pages 1272–1282, San Francisco, CA, USA, April 2003.

[6] P. Michiardi and R. Molva. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Proceedings of the IFIP TC6/TC11 6th Joint Working Conference on Communications and Multimedia Security*, pages 107–121, 2002.