Czech Technical University in Prague
Faculty of Electrical Engineering
Department of Computer Science & Engineering

Review of the PhD. thesis

Trust Management Systems in P2P Networks

submitted by

Mgr. Miroslav Novotný

The main goal of the doctoral thesis submitted by Mgr. Miroslav Novotný has been to create an efficient approach to security aspects of distributed application that are utilizing P2P networking technology. On the basis of the analysis of existing systems, which are able to detect malicious peers in P2P based applications, he developed the new trust management system (TMS) BubbleTrust. The other part of the thesis is description of the simulator P2PTrustSim, which has been developed together with BubbleTrust, and has been used for comparison of BubbleTrust with some existing TMS systems.

The BubbleTrust algorithm supports trust managements for a set of peers, which are combining the consumer and provider role. Such an approach means much higher complexity for the area of distributed application then more simpler client-server approach for P2P file systems. Trust management is implemented by the algorithm, which alternates provider rating and evaluator rating functions in peers of the bubble subset (?).

I really would appreciate some description of the bubble idea presented graphically in the Fig.7 in relation to the network topology and to the DHT node key identification.

The algorithm works generally for restricted number of peers, however, examples in simulation show results for thousands peers. It would be possible presenting an example of corresponding distributed application in current cloud/P2P networks?

The BubbleTrust peers are storing relations locally and in the DHT database. Is there any relation of the BubbleTrust with the DHT method used (e.g. Pastry utilised as the P2PTrustSim basis)?

The provider and evaluator functions $pv(x_1, x_2)$ $ev(x_1, x_2)$ are using parameters T_p and T_e (Zipf's law), can be the usage of T_p and T_e more explicitly explained?

The simulator is based on FreePastry DHT and it is able comparing BubbleTrust and six other selected TMS methods. The testing has been done on different malicious strategies and proved the high advantage of BubbleTrust. The testing covered rather large percentage of malicious peers (40%).

The two different dynamic criterions' simulations are based on the adding of all malicious peers to the application at the same time, and on changing of the high percentage of peers' behaviour (from honest into malicious) simultaneously. Such a step produces the high burden for any TMS. Is the simulator able to evaluate TMS functions for sequential changes of peer behaviour as well?

Another question related to BubbleTrust and P2PTrustSim: would be reasonable for the peer to use the TMS information about its malicious evaluation as an information for its behaviour change (e.g. improvement/modification of its behaviour to the honest evaluation)?

All simulations have been done in steps of 10 minutes. Is the synchronous behaviour necessary for the BubbleTrust or can be the asynchrony of some level accepted?

The results related to the presented BubbleTrust trust management method have been published in conferences with high level distribution of papers (Springer book series, IEEEExplore).

To conclude, although I had some notes to the text of the thesis, I can assert, that the thesis solves important and timely topics, it presents well the ability of its author, Mgr. Miroslav Novotný, to work in the very interesting area of the security of distributed applications (in P2P/clouds), and that the results presented in the thesis could create a good area for the future research and implementation of specific areas in cloud computing.

I can fully recommend the thesis, in the interpretation of the Law 111/98 in the Digest, for the defence and judge the candidate worthy to be awarded by the PhD. degree in Software Engineering at the Faculty of Mathematics and Physics of Charles University in Prague.

Prague, 20th August, 2012

doc. Ing. Jan Janeček, CSc.