Neighbor Similarity Trust against Sybil Attack in P2P E-commerce

Authors: Musau, F. ; Sch. of Inf. Sci. & Eng., Central South Univ., Changsha, China ; Guojun Wang ; Song Guo ; Abdullahi, M.B.

Abstract

Peer to peer (P2P) e-commerce applications exist at the edge of the Internet with vulnerabilities to passive and active attacks. These attacks have pushed away potential business firms and individuals whose aim is to get the best benefit in e-commerce with minimal losses. The attacks occur during interactions between the trading peers as a transaction takes place. In this paper, we propose how to address Sybil attack, which is a kind of active attack. The peers can have bogus and multiple identity to fake their own ones. Most existing work, which concentrates on social networks and trusted certification, has not been able to prevent Sybil attack peers from participating in transactions. Our work exploits the neighbor similarity trust relationship to address Sybil attack. In this approach, referred to as Sybil Trust, duplicated Sybil attack peers can be recognized as the neighbor peers become acquainted and hence more trusted to each other. Security and performance analysis shows Sybil attack can be minimized by our proposed neighbor similarity trust.

Published in:

Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC), 2012 9th International Conference ,Date of Conference:4-7 Sept. 2012,Page(s):547 - 554,Print ISBN:978-1-4673-3084-8

Author keywords:

P2P,Sybil attack,collusion attack,neighbor similarity,trust