Computer Communications 35 (2012) 608–618

Contents lists available at SciVerse ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

# A distributed reputation and trust management scheme for mobile peer-to-peer networks

Basit Qureshi, Geyong Min *, Demetres Kouvatsos

*School of Computing, Informatics and Media, University of Bradford, Bradford BD7 1DP, UK*

ARTICLE INFO

*Article history:*
Available online 12 August 2011

*Keywords:*
Trust management
Trust ratings aggregation
Mobile P2P systems
Wireless ad-hoc networks

ABSTRACT

In peer-to-peer (P2P) networks, trust ratings aggregation and peer ranking are unreliable, time-consuming and space-demanding operations. The swift expansion of emerging P2P techniques towards the domain of mobile computing poses significant challenges for trust and security management. Several trust management schemes have been proposed recently to counter the security threat on P2P systems. However, due to the difficulties caused by system mobility and dynamic network topology, there is an increasing requirement of decentralized and distributed trust management schemes. In this paper, we initially investigate and analyze four typical decentralized and distributed trust management schemes. Based on the findings of this analysis, a robust distributed reputation and trust management scheme, referred to as M-trust, is proposed for mobile P2P networks. The new scheme utilizes confidence in reputation, based on interactions among peers, to reduce the computation complexity. Furthermore, distributed algorithms are presented for accurate and reliable trust ratings aggregation and space management. The performance of M-trust is evaluated in comparison to the existing schemes using extensive simulation experiments. The results demonstrate that M-trust possesses the excellent overall performance in terms of accuracy, reliability, convergence speed, and detection rate under various constraints of mobility, trust threshold and network out-degree.



## 1. Introduction

The swift growth of peer-to-peer (P2P) services such as file sharing, social networking and content retrieval has been recently expanded to the domain of wireless mobile systems. The materialization of mobile services on wireless networks and the rapid proliferation of portable devices have stimulated a general trend towards extending P2P characteristics to mobile computing environments. As a result, the P2P paradigm has migrated to pervasive computing scenarios. Since P2P systems do not have the central administration and peers are autonomous, some of the peers are intrinsically insecure and untrustworthy [1,2]. To handle the trustworthiness issues of such systems in open and decentralized environments, trust and reputation schemes are adopted to establish trust between peers. In a trust and reputation system, the historical behaviors and activities are recorded for each peer. The statistics of these behaviors and activities are used to predict how a peer is likely to behave in the future [3].

Many studies [4–28] have developed the decentralized trust and reputation systems and addressed various issues of trust and reputation management. For instance, FIRE, discussed in [10], is a decentralized trust and reputation model for P2P systems. Rule-based trust management schemes proposed in [13,14] and pseudo-trust presented in [15] address the significance of the initial trust values for rule-based trust management schemes. Moreover, several studies [12,16–19] have contributed to the framework design and middleware architecture for trust management.

In large-scale P2P networks, trust ratings aggregation and peer ranking are unreliable, time-consuming and space-demanding operations. Processing massive trust and reputation information to compute up-to-date trust ratings for peers requires extensive computation power as well as large storage space. Peers are not always honest in their interactions and may provide inaccurate or false trust ratings for other peers. The presence of malicious peers and unreliable sources in the network, if undetected, can lead to inclusion of unrealistic trust ratings in the computation process, therefore deteriorating the accuracy and system performance. Recent work presented in [9] provides a gossip-based trust ratings aggregation scheme for structured P2P networks. This scheme utilizes bloom filters for reputation ranking and storage. Although the presented technique is effective in trust ratings aggregation with the low computation complexity, it is applicable to fixed P2P networks but unsuitable for the mobile P2P environment. Similar techniques, such as H-trust [11] and Fuzzy trust [12], improve

* Corresponding author.
*E-mail addresses:* b.qureshi@bradford.ac.uk (B. Qureshi), g.min@bradford.ac.uk (G. Min), d.kouvatsos@bradford.ac.uk (D. Kouvatsos).

0140-3664/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2011.07.008

the efficiency of reputation aggregation for trust ratings, but fail to address the mobility issue in mobile P2P networks.

Mobile P2P networks pose greater challenges in trust management due to the frequent changes in network topology. To deploy a mobile P2P system a straightforward approach is to mount a P2P architecture over Mobile Ad hoc Networks (MANETs) [2] where the transitory sets of mobile nodes dynamically establish their own network on the fly. Nodes in a MANET are constrained by a limited amount of energy, storage, bandwidth and computational power. These limitations prove to be a hindrance in seamless connectivity with other peers and thus deteriorating the effectiveness of many trust and reputation schemes. Since a reputation-based system requires trust ratings from other peers to evaluate or update trust scores, it is imperative that the trust management system should be decentralized and can effectively aggregate trust ratings despite of delays, connection loss and malicious behavior from peers [29–34]. Moreover, as it is impossible to establish the global trust ratings for peers, any trust management scheme for mobile P2P systems must take into account trust ratings at a local level and build the reputation of peers based on accumulated ratings.

This paper presents a distributed reputation and trust management scheme, referred to as M-trust, in mobile P2P networks. To this end, we first investigate the effectiveness of various decentralized trust ratings aggregation schemes in MANETs. Specifically, the typical trust management schemes including the received ratings aggregation [20], weighted average of ratings [10], Bellman–Ford based algorithm [21], total and ultimate trust scheme [22] are thoroughly investigated and compared. Based on the analytical results, an efficient, accurate, robust, scalable and light-weight reputation aggregation and trust management scheme is proposed for mobile P2P networks.

M-trust incorporates distributed trust rating aggregation algorithms that acquire trust ratings from direct and witness recommendations from distant nodes, rapidly and accurately. The proposed scheme utilizes confidence in reputation, based on interactions among peers, to decrease the time required in computing trust ratings and reduce the space for storing trust ratings. The results obtained from extensive simulations show that M-trust is effective compared to the existing techniques for various performance metrics such as accuracy, reliability, convergence speed, rate of detecting malicious peers under different constraints of mobility, trust threshold, network out-degree and global aggregation error rate.

The rest of this paper is organized as follows. Section 2 presents and compares the typical schemes for trust ratings aggregation. Section 3 describes the proposed scheme followed by the detailed analysis and comparison of performance results in Section 4. Section 5 concludes this work.

## 2. Comparison and analysis of the existing trust schemes

In the open and decentralized P2P environment, peers do not have any centralized authority to maintain and distribute reputation information. A full-aggregation reputation system calculates the reputation score of a peer by considering the opinions from other peers that have interacted directly or indirectly with this peer. Usually a full-aggregation reputation approach is of high accuracy, but has heavy overload in unstructured large-scale P2P networks. In addition, the reputation convergence is not fast enough. However, in the selective-aggregation systems, reputation ratings are derived from a subset of the existing opinions in distributed P2P networks. In mobile P2P networks, users with a higher trust level have the luxury to stay connected for a longer period and communicate with a large number of users. Such users are able to store and forward data from adjacent nodes while serving as an intermediate router. In what follows, we will present and compare several typical trust schemes including received ratings aggregation [20], weighted average of ratings [10], Bellman–Ford based algorithm [21], and total and ultimate trust scheme [22] for trust ratings aggregation. For the purpose of clarity and quick reference, Table 1 summarizes the notations and the corresponding definitions.

Fig. 1 illustrates a trust overlay network. The vertices in the graph correspond to peers/nodes in the network. An edge between peers $A$ and $B$ represents a connection between the peers if and only if $A$ is a client of $B$ in *direct interaction*. The real number $r \in [0,1]$ reflects how much $A$ trusts $B$ ($T_{AB} = 0$ means that $A$ considers $B$ as untrustworthy; $T_{AB} = 1$ indicates that $A$ fully trusts $B$). As opposed to direct interaction trust, *witness interaction* trust is used to compute trust of a peer if no direct connection exists. In this case, all nodes that have a direct interaction with the evaluator node are asked to provide a trust rating for the target node.

As an example in Fig. 1, $B$ has a direct trust interaction with $A$ and $D$. If $B$ seeks trust ratings for node F, it forwards the request to immediate neighbors $A$ and $D$. Since $D$ has a direct interaction with $F$, $D$ can provide the trust rating for $F$. It is worth noting that $A$ may have trust ratings for $F$ made available through a longer path ($B \rightarrow A \rightarrow C \rightarrow F$). All local and received trust ratings are stored in a table called trust list, *t_list*.

### 2.1. Received ratings aggregation

In the received ratings aggregation scheme [20], if the intermediate node providing trust ratings has a high trust score ($\tau_{ij} > trust\_threshold$), the local peer's ratings are overwritten with the ratings provided by the intermediate node. The following equation can be used to calculate trust ratings of this method.

$$\tau_{ik} = \begin{cases} \tau_{ij}\tau_{ij} \geqslant threshold \\ \tau_{ij} * \tau_{jk}\tau_{ij} < threshold \end{cases} \quad (1)$$

As an example shown in Fig. 2, node $B$ receives ratings for $C$ from $A$. If the *trust_threshold* is set to be 0.4, since $T_{AB} = 0.6$ is larger than the *trust_threshold* value, the ratings provided by node $A$ can be trusted. Node $B$ subsequently updates/overwrites its own rating for $C$ to 0.8. In the case that the trust ratings for witness node is less than the *trust_threshold*, the two ratings are multiplied and the result is stored in the local trust list, (e.g. if $\tau_{AB} = 0.2$ then new

**Table 1**
List of notations.

| Notation | Description |
|---|---|
| *t_list* | List of all trust ratings |
| BF | Bellman–Ford algorithm |
| MT | M-Trust rating aggregation |
| UT | Ultimate trust scheme |
| WA | Weighted Average trust management scheme |
| RR | Received Ratings trust management scheme |
| $D$ | Degree of connectivity |
| $\gamma$ | Trust confidence |
| $\alpha$ | Number of positive interactions |
| $\beta$ | Number of negative interactions |
| $\tau_{ij}$ | Trust rating of peer $j$ for $i$ using RR |
| $\varphi_{ij}$ | Trust rating of peer $j$ for $i$ using WA |
| $\omega_{ij}$ | Trust rating of peer $j$ for $i$ using BF |
| $U_{ij}$ | Trust rating of peer $j$ for $i$ using UT |
| $\mathcal{M}_{ij}$ | Trust rating of peer $j$ for $i$ using MT |
| $C_x$ | Congregation state |
| $N_x$ | Number of nodes in the simulation |
| $T_{ij}$ | Local trust rating of peer $j$ for $i$ |
| $\Theta$ | Percentage of malicious peers |
| E | Aggregation error |
| $G_{ij}$ | Global trust rating of peer $j$ for $i$ |