Available online at www.sciencedirect.com

ScienceDirect

IERI Procedia 10 (2014) 45 – 50

Procedia IERI

www.elsevier.com/locate/procedia

2014 International Conference on Future Information Engineering

Improvement of the Byzantine Agreement Problem under Mobile P2P Network

Hui-Ching Hsieh[a], Mao-Lun Chiang[b]

[a]Department of Information Communication, Hsing Wu University, New Taipei City, Taiwan, R.O.C.
[b]Department of Information and Communication Engineering, Chaoyang University of Technology, Taichung County, Taiwan, R.O.C.

Abstract

For improving the accuracy under P2P networks, it must be assured that all non-faulty peers can reach agreement. As such, all the non-faulty peers need to work collaboratively despite disturbances caused by faulty peers. This agreement issue is usually called as the Byzantine Agreement (BA) problem. In previous works, $\lfloor (n\text{-}1)/3 \rfloor + 1$ bouts for exchanging message are necessary to allow all non-faulty peers reaching an agreement. Furthermore, the message complexity of these algorithms are $O(n^n)$. Hence, the relevant algorithms are not suitable for mobile P2P networks in which there may have a great quantity of mobile peers. In this study, a more efficient algorithm has been proposed to decrease the required bouts for exchanging message. Our proposed algorithm only need to run three bouts for exchanging message to allow all non-faulty peers to reach an agreement despite some peers roaming among the different network. It also can decrease the message complexity to $O(n^2)$. It is more suitable and efficient than previous efforts aimed at the mobile P2P network.

Selection and peer review under responsibility of Information Engineering Research Institute

Keywords: Byzantine Agreement problem; fault-tolerance; distributed system; mobile P2P network

1. Introduction

Mobile Peer-to-Peer (P2P) networks can be defined as a distributed system comprised of a great quantity of peers. Basically, the accomplishments of mobile P2P network depend upon the ability to spread content efficiently and correctly by utilizing the transmission capacity and cooperation of all peers. Thus, a mobile P2P network has the ability to serve large numbers of peers based on the good service quality [1] under the

Selection and peer review under responsibility of Information Engineering Research Institute
doi:10.1016/j.ieri.2014.09.089

indispensable condition that all peers can reach agreement and cooperate well in the network. Unfortunately, in the real situation, there may have some faulty peers to disturb the cooperation between peers. These faulty peers may do some activities to degrade the network performance. Hence, it's important to propose an algorithm to assure the correctness of the network system even if there have some faulty peers.

In the past, there have many fault tolerance schemes been studied, in which the agreement algorithms has attracted much attention. Basically, there have many algorithms [2][3][4][5][7][9][10][11] been proposed for processors to reach agreement or for security applications in a distributed system despite failed processors. This kind of unanimity problem is defined as the Byzantine Agreement problem (BA problem) [5], and was originally proposed by Lamport et al in 1982. Basically, the proposed algorithm must reach the following agreement and validity requirements:

- Agreement: It means that all non-faulty processors need to agree on a unanimity value;
- Validity: It means that the final common value v must equal to the start's initial value, if the starter processor is non-faulty.

Unfortunately, the previous algorithms [6][8][10] require $\lfloor (n\text{-}1)/3 \rfloor + 1$ bouts for exchanging message. Furthermore, the complexity with message will be $O(n^n)$. These algorithms cannot be applied for mobile P2P networks since it may include millions of peers, resulting in a great quantity of overhead while exchanging message.

Besides, peers can roam between different mobile P2P networks without disrupting the execution of the applications arbitrarily. The previous BA algorithms can reach agreement under the pre-defined network topologies [6][8][10]. However, network technology continues to grow quickly and applications in mobile P2P networks recently have reached high complexity. In other words, the previous algorithms cannot make all non-faulty peers to reach an agreement when there have peers roam around the network. Thus, the traditional algorithms [6][8][10] are unsuitable for mobile P2P networks. The agreement problem must be revised under the mobile P2P network.

In order to make the BA algorithm more suitable for mobile P2P network, we revisit and propose a new algorithm: Byzantine Agreement algorithm for Mobile P2P network (BAMP2P), to ensure all peers get an agreement result within three bouts for exchanging message while tolerating the largest quantity of faulty peers.

The rest of this article is presented as follows: The details of BAMP2P are given in Section 2. The correctness is shown in Section 3, and the conclusions are shown in Section 4.

2. The proposed algorithm BAMP2P

In general, each non-faulty peer will execute the same algorithm BAMP2P simultaneously to reach agreement, and BAMP2P includes two phases of works: the exchanging message phase and the making decision phase.

Here, all non-faulty peers must execute three bouts for exchanging message to collect sufficient messages to reach agreement. Noticeably, some peers may roam the network during the execution of BAMP2P. We suppose that all peers can only roam in the network while executing the exchanging message phase. It's due to the reason that there has no message exchange activity during the period of making decision phase. If peers can roam about at that period of time, peers will not have enough messages to reach an agreement correctly. In other words, if the algorithm allows peers roaming about the network during the making decision phase, there will be insufficient messages for peers to determine reliable peers and to reach agreement correctly. Thus, this assumption is needed to assure that all peers have sufficient information to determine reliable peers and to avoid interrupting this process. The BAMP2P procedure is stated below and described by Fig. 1.

Exchanging message Phase: