Chapter 11
Token Based Mutual Exclusion in Peer-to-Peer Systems

Mayank Singh
ABV-Indian Institute of Information Technology and Management, India

Shashikala Tapaswi
ABV-Indian Institute of Information Technology and Management, India

ABSTRACT

Mutual exclusion is one of the well-studied fundamental primitives in distributed systems, and a number of vital solutions have been proposed to achieve the same. However, the emerging Peer to Peer systems bring forward several challenges to protect consistent and concurrent access to shared resources, as classical peer-to-peer systems, like Napster, Gnutella, et cetera, have been mainly used for sharing files with read only permission. In this chapter, the authors propose a quorum based mutual exclusion algorithm that can be used over any Peer to Peer Distributed Hash Table (DHT). The proposed approach can be seen as extension to traditional Sigma protocol for mutual exclusion in Peer to Peer systems. The basic idea is to reduce message overhead with use of smart nodes present in each quorum set and message passing between the current owners of resource with next resource requester nodes.

INTRODUCTION

Over the past several years, peer-to-peer systems have generated many headlines across several application domains. The increased popularity of these systems has led researchers to study their overall performance and their impact on the underlying Internet. The unanticipated growth in popularity of peer-to-peer (P2P) systems has raised a number of significant problems. Mutual Exclusion is one of such problems which has not been yet been thoroughly studied in the P2P domain. It is crucial for design of P2P systems. Many problems involving replicated data, computational resources etc. require mutual exclusion.

The problem of mutual exclusion can be described as a collection of asynchronous processes, each alternately executing a critical and a

DOI: 10.4018/978-1-4666-0203-8.ch011

non-critical section that must be synchronized so that no two processes ever execute their critical sections concurrently. It was first described and solved by Dijkstra in (Dijkstra, 1965). Distributed mutual exclusion introduces some new requirements which can be summarized as follows:

- **Safety:** At most one process may execute in critical section at any time.
- **Liveness:** Every request for a critical section is eventually granted.

Even though mutual exclusion is a classical, well studied problem in distributed systems and several viable solutions have been proposed, it yet remains to be completely explored in the P2P domain. Directly adapting the mutual exclusion algorithms from distributed computing literature is not possible due to the differences in the underlying system models, one of which is the absence of any centralized index server to keep track of membership and to ensure consistency. Classical decentralized algorithms use several rounds of all-to-all communication which is unscalable. Mutual exclusion algorithms that currently exist do not have scalability and efficiency, which makes their applicability limited. This gives rise to new challenges that need to be tackled in order for this field to become successful in the future.

Today P2P and the Grid are in the same developmental stage, as traditional distributed systems were about a decade ago. Concepts like scalability and fault-tolerance need to be reworked for this new generation of distributed environment. One of the fundamental obstacles to overcome is to provide a mechanism to share resources transparently and efficiently across a large number of independent hosts. Resources can be either computational resources or data, and access to them should be controlled in a completely decentralized manner, even in the presence of high churn.

Since each resource can have multiple replicas, the problem in question becomes even more challenging. Access to that resource is controlled by a set of replicas. In order to access it, majority of the replicas must reach a consensus. The concept of a quorum set is defined to be a group of nodes such that the intersection of any two quorum sets must not be empty. A token ring approach to mutual exclusion is one where all the nodes are arranged in a ring formation and a token is constantly circulated. When a node acquires the token from its neighbor it checks to see if it is attempting to enter a critical region. If so, it enters the region, does all the work it needs to and leaves the region. Token is then passed to the next node in the ring.

The main contribution of this study is the design and discussion of a proposed protocol for achieving mutual exclusion in dynamic P2P systems. This goal is accomplished while maintaining a low message overhead and reducing the burden on the replicas of controlling access to the critical section, by distributing the load evenly among the quorum set nodes. Another important contribution is its ability to be incorporated with any generic P2P DHT (Stoica, 2001), (Ratnasamy, Francis, Handley, Karp, & Shenker, 2001), depending on the application requirements.

A mutual exclusion algorithm must satisfy the following requirements (Velazquez, 1993):

- At most one process can execute its critical section at a given time.
- If no process is in its critical section, any process requesting to enter its critical section must be allowed to do so in finite time.
- When competing processes concurrently request to enter their respective critical sections, the selection cannot be postponed indefinitely.
- A requesting process cannot be prevented by another one to enter its critical section within a finite delay.