Journal of Computer Engineering and Information Technology

Commentary A SCITECHNOL JOURNAL

Study of Election Algorithms on the Basis of Message Passing Approach

Mehrnoosh Asadi*

Department of Computer Engineering, University of Lucknow, Lucknow, Uttar Pradesh, India

***Corresponding author:** Mehrnoosh Asadi, Department of Computer Engineering, University of Lucknow, Lucknow, Uttar Pradesh, India.E-mail: asadinoosh@gmail.com

Received date: 03 June, 2022, Manuscript No. JCEIT-22-61672;

Editor assigned date: 06 June, 2022, PreQC No. JCEIT-22-61672(PQ);

Reviewed date: 15 June, 2022, QC No JCEIT-22-61672;

Revised date: 13 July, 2022, Manuscript No. JCEIT-22-61672(R);

Published date: 22 July, 2022, DOI:10.4172/jceit.1000237.

Description

An important challenge in distributed systems is the adoption of suitable and efficient algorithms for coordination selection. The leader election is important problem in distributed system as data is distributed among different node which is geographically separate. For maintaining co-ordination between the node, leader node have to be selected. The main role of an elected coordinator is to manage the use of shared resources in optimal manner. This paper represents the different election algorithms with their limitations as well comparative analysis of them, efficiency in terms of number of messages exchanged in each case and the complexity of various coordinator selection algorithms in distributed systems. Distributed system, Election, Coordinator, Priority. In a distributed computing system, a node is used to coordinate many tasks. It is not an issue which node is doing the task, but there must be a coordinator that will work at any time. An election algorithm is an algorithm for solving the coordinator election problem. Various algorithms require a set of peer nodes to elect a leader or a coordinator. Elections may be needed when the system is initialized, or if the coordinator crashes or retires. A Distributed system is a collection of autonomous computing nodes which can communicate with each other and which cooperate on a common goal or task. Tanenbaum and van Renesse: A distributed system is one that looks to its users like an ordinary, centralized, system but runs on multiple independent CPUs. A distributed system is a collection of processors interconnected by a communication network in which each processor has its own local memory and other peripherals and the communication between them is held by message passing over the communication network.

Algorithm Sequence of Actions

Several distributed algorithms require that there be a coordinator node in the entire system that performs some type of coordination activity needed for the smooth running of other nodes in the system. As the nodes in the system need to interact with the coordinator node, they all must unanimously who the coordinator is. Also if the coordinator node fails due to some reason then a new coordinator node must be elected to take the job of the failed coordinator. It is a synchronous system and it uses timeout Mechanism to keep track of coordinator failure detection. Each node has a unique number to distinguish them. Every node knows the node number of all other nodes. Nodes do not know which nodes are currently up and which nodes are currently down. In the election, a node with the highest node number is elected as a coordinator which is agreed by other alive nodes. A failed node can re-join in the system after recovery. In this algorithm, there are three types of message and there is an election message (ELECTION) which is sent to announce an election, an answer (OK) message is sent as response to an election message and a coordinator (COORDINATOR) Message is sent to announce the new coordinator among all other alive nodes . When a node P determines that the current coordinators crashed because of message timeouts or failure of the coordinator to initiate a handshake, it executes bully election. All the nodes in the system are organized as a logical ring. The ring is unidirectional in the nodes so that all the messages related to election algorithm are always passed only in one direction.

The message circulates over the ring, if the successor of the sender nodes is down the sender can skip over successor, or the one after that until an active member is located. When a node n1 sends a request message to the current coordinator and does not receive a reply within a fixed timeout period, it assumes that the coordinator has crashed. So it initiates an election by sending an election message to its successor. This message contains the priority of node n1. On receiving the election message, the successor appends its own priority number to the message and passes it on to the next active member in the ring. In this manner, the election message circulates over the ring from one active node to another and eventually returns back to node n1. Node n1 recognizes the message as its own election message by seeing that in the list of priority numbers held within the message the first priority number is its own. Among this list, it elects the node with the highest priority as the new coordinator and then circulates a coordinator message over the ring to inform the other active nodes. When the coordinator message comes back to node n1, it is removed by node n1. When a node n2 recovers after failure, it creates an inquiry message and sends it to its successor. The message contains the identity of node n2. If the successor is not the current coordinator it simply forwards the enquiry message to its own successor. In this way, the inquiry message moves forward along the ring until it reaches the current coordinator. On receiving the inquiry message, the current coordinator sends a reply to node n2 informing that it is the current coordinator. There are five types of message. An election message is sent to announce an election, an ok message is sent in response to an election message, on recovery, a process sends a query message to the processes with process number higher than it to know who the new coordinator is, a process gets an answer message from any process numbered higher than it in response to a query message and a coordinator message is sent to announce the number of the elected process as the new coordinator.

Cryptographic Protocols

Cloud data can be very large text-based or scientific applications, unstructured or semi-structured, and typically append-only with rare updates cloud data management an important research topic in cloud computing. Since service providers typically do not have access to the physical security system of data centres, they must rely on the infrastructure provider to achieve full data security. Even for a virtual private cloud, the service provider can only specify the security setting remotely, without knowing whether it is fully implemented. The infrastructure provider, in this context, must achieve the objectives

like confidentiality, auditability. Confidentiality, for secure data access and transfer, and auditability, for attesting whether security setting of applications has been tampered or not. Confidentiality is usually achieved using cryptographic protocols, whereas auditability can be achieved using remote attestation techniques. However, in a virtualized environment like the clouds, VMs can dynamically migrate from one location to another; hence directly using remote attestation is not sufficient. In this case, it is critical to build trust mechanisms at every architectural layer of the cloud. Software frameworks such as MapReduce and its various implementations such as Hadoop are designed for distributed processing of data-intensive tasks; these frameworks typically operate on Internet-scale file systems such as GFS and HDFS. These file systems are different from traditional distributed file systems in their storage structure, access pattern and application programming interface. In particular, they do not implement the standard POSIX interface, and therefore introduce compatibility issues with legacy file systems and applications. Several research efforts have studied this problem.

Encryption is a key technology for data security. Understand data in motion and data at rest encryption. Remember, security can range from simple easy to manage, low cost and quite frankly, not very secure all the way to highly secure very complex, expensive to manage, and quite limiting in terms of access. You and the provider of your Cloud computing solution have many decisions and options to consider. For example, do the Web services APIs that you use to access the cloud, either programmatically, or with clients written to those APIs, provide SSL encryption for access, this is generally considered to be a standard. Applications are not hardware specific; various programs may run on one machine using virtualization or many machines may run one program. Virtualization can provide significant benefits in cloud computing by enabling virtual machine migration to balance load across the data center. In addition, virtual machine migration enables robust and highly responsive provisioning in data centres. Virtual machine migration has evolved from process migration techniques.