**BFT-SMART：**

BFT-SMaRt is a Java-based open source library that implements a robust BFT state machine replication system similar to the PBFT protocol. It provides a BFT protocol process that can tolerate Byzantine attacks and a CFT protocol process that is non-Byzantine attack (crash fault tolerance).

The following content is the implementation of the specific functional modules of BFT-SMART, and each module of BFT-MART is analyzed according to the sequence of the library package：

1. clientsmanagement：The function of this module is to sort and pack the information transmitted by the client into blocks according to the client id classification. The three most important function of this module are: 1) function requestReceived: The copy obtains the request message to be agreed by the client from the netty framework, After inspection and verification, submit the message to the client data ClientData, start the timer, and wait for the master node to start the consensus; 2) function getPendingRequests: The replica master node calls it when a round of consensus is started to obtain the current message to be agreed upon (already according to the time). Sort messages packaged into blocks); 3) function requestsOrdered: The replica ends at the three-stage BFT consensus. During the reply stage, the replica deletes the message to be sorted from the linked list and adds it to the sorted linked list at the same time.
2. communication：The communication module is the guarantee for a reliable and authenticated p2p channel in a distributed network.

* Establish mutually trusted Java Socket IO connections between server to realize point-to-point message processing.
* A Netty NIO connection with higher robustness and higher availability is established between the server and the client to realize large-scale message processing.

The work of the local server node communication system is mainly maintained by the thread ServerCommunicationSystem.java, which encapsulates the communication process between the underlying nodes (typical: send sending method, receive receiving method). (Message Type: Consensus / View Switch / State Transfer).

Server：The communication between replicas uses p2p socket IO, and each server generates corresponding node parameters according to the processId of the parameters. Each server use a thread to send and receive.

Client：Communication between the client and the server is established through Netty.

3、consensus：This is one of the most important modules of the SMR system. BFTSMART improves on BFT-like consensus protocols similar to PBFT.

The consensus module is divided into two roles: 1) Proposer: This module realizes the role of the node as the leader. When the replica acts as the proposer, it will act as the leader of the consensus, process the messages to be consensus and start a new round of consensus; 2) The module implements the core of the consensus algorithm: PROPOSE, ACCEPT, and WRITE messages are processed and generated here.

图示, 工程绘图

描述已自动生成

1. tom（Total Order Multicast）：This module includes the implementation of the api interface, the leaderchange protocol and the basic process of SMR. The replica obtains the pending messages received by the client, calls startConsensus of the Proposer module to start the consensus instance, and creates and destroys timers for the pending messages of each client when the message is received.
2. reconfiguration：The reconfiguration protocol is implemented in this module

An additional reconfiguration protocol is provided in the BFT-SMART library that modifies the current view of the system, CurrentView, at runtime, i.e. copies can be added or removed without stopping the system. To achieve this, a special type of client (TTP) called View Manager(trusted third party) is used in BFT-SMART, select a reliable third party or system administrator to add/remove nodes to the current view, when other replicas receive VMMessage message, the CurrentView is updated.

The scheme using the threshold signature mainly modifies the consensus package and the tom package.Now,We use Practical Threshold Signatures scheme. The specific directory is in bftsmart.tom.util.thresholdsig or bftsmart. reconfiguration.util.thresholdsig(I think it should be placed on bftsmart.tom.util.thresholdsig)

Mainly modified the consensus package, focusing on the role package. We define two roles : primary and backup. primary is used to start consensus and aggregate signatures.backup verifies the message, signs it with threshold signing key, and monitors the behavior of the primary.

The position of the viewchange module is in tom.core.ExecutionManager.java 、tom.core.synchronizer and tom.leaderchange package.

图形用户界面

低可信度描述已自动生成