A Voting Mechanism for Virtual Dynamic Role Node Groups

-- Proof Of Virtual Dynamic Role Groups(POVDRG)

Robert Xu 20180525

Problem Description：

In an open system with multiple nodes participating, if you need to vote for any propositions, there will be two problems:
1. Problems outside the system - Including how do nodes entering and exiting the system and the attacking from outside;
2. Problems inside the system - Contains whether the internal nodes are stable, trustworthy, and whether the communication between the nodes is stable to ensure the complete transmission of information.

Problem Analysis：

1. There is a significant plateau for a single node in the transmission network bandwidth, hardware calculation, and hardware storage , so that the node has limited viability;
2. It should be considered that the effect on the overall stability of the nodes system when a node enters the system and exits the system;
3. It should be considered how to ensure the stability of the internal nodes, because the internal nodes are essentially physical;
4. Nodes may show dishonesty or attack other nodes due to human manipulation;
5. How to ensure the communication between nodes is complete and efficient;
6. What is the future evolution direction of the system.

Existing technology solutions：

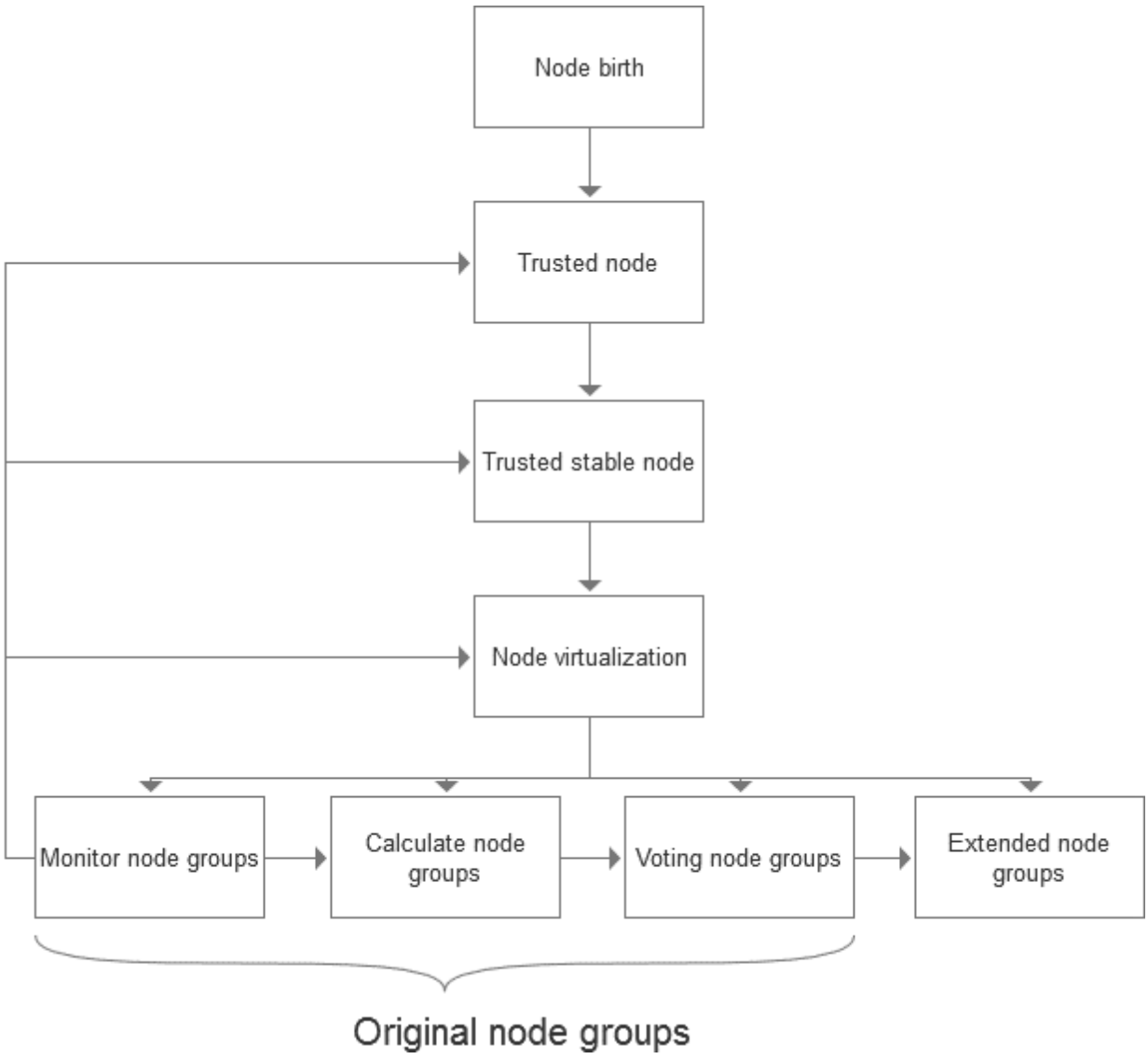
1. It is often use virtual cloud nodes to replace the physical nodes, cloud nodes can infinitely increase hardware computing capabilities and storage capabilities in the technical theory. In addition, the current cloud node is easily located by unauthenticated visitors such as DDos attackers due to the visibility of the node, so node protection and visitor review become an option;
2. External nodes can enter the node system through a standard rule, and the node exit system has many way such as active exit, passive disconnection, network interruption, power failure, etc. The

management of the node system needs to consider the extreme situation in which a large number of nodes are quickly disconnected. There should be an efficient seed-recovery mechanism in the system;

3. Since the internal nodes are controlled by humans, while distributing network security design, it is need to design a mechanism to encourage each node to maintain stability. The existing consensus mechanisms include Proof of Work, Proof of Stake, Delegated Proof of Stake and other consensus to motivate the participating nodes, which allows the stability of the node to be supported by rational people and rational behavior;
4. The current system protection mechanism is setting the cost of violations so that participants can remain rational and will not attack the system. However, due to the uncontrollability of human nature, it must be considered that people may violate the regulations rationally or irrationally in the system. An attacker may control a large number of accounts to attack at any cost, and even influence the stability of the system through double-loss attacks. So that a stable system should be a personal uncontrollable system(PUS). The big data analysis technology can be used for data acquisition, and to make credibility judgments through the node behavior. An untrusted node will quickly lose its own voting weight and even be cleared out of the system;
5. 5, TCP protocol has become an effective solution in many years of application. At the same time, each node's communication can achieve complete information with the path identifiers, and the transmission efficiency in the system is related to the way of communication transmission.
6. As a self-managed system with an incentive mechanism, it is very important to maintain scalability. The future evolution direction of the system will conform to the characteristics of the human population and the division of labor of the nodes will continue to be refined and multidimensional.

A reasonable technical solution：

Node Virtualization + Node Role Extension + Dynamic Full Node + Behavior Monitoring Trusted Role + Node Communication Identity



The roles of the node under the trusted voting mechanism

1. Judging trusted nodes

Trusted node calculation model:

a) the function of generating node behavior

Set the node's behavior time to t and the behavior action to Ai, then a node's behavior can be expressed as ∑(t,i)Ai. Where t is the irreversible time increment;

b) Calculate the similarity of the behavior of two nodes

Method: Mapping the behavior of two nodes in the same time period into vector space and calculate the cosine approximation of the two groups of behaviors after calculating the action frequency.

Suppose the action of the A node is the vector A = (A1, A2,..., An). The action of node B is B = (B1,B2,...,Bn). The vector cosine between these two actions is:

$$\cos\theta = \frac{\sum_1^n (A_i \times B_i)}{\sqrt{\sum_1^n A_i^2} \times \sqrt{\sum_1^n B_i^2}}$$

The range of cos θ is [-1, 1]. When cos θ is close to 1, it means that the two behaviors are similar.

c) Select node

The node with exactly the same behavior is only counted once. The node received at the last moment of calculation is the standard node, and the remaining nodes are removed from the system.

d) Dynamic adjustment period

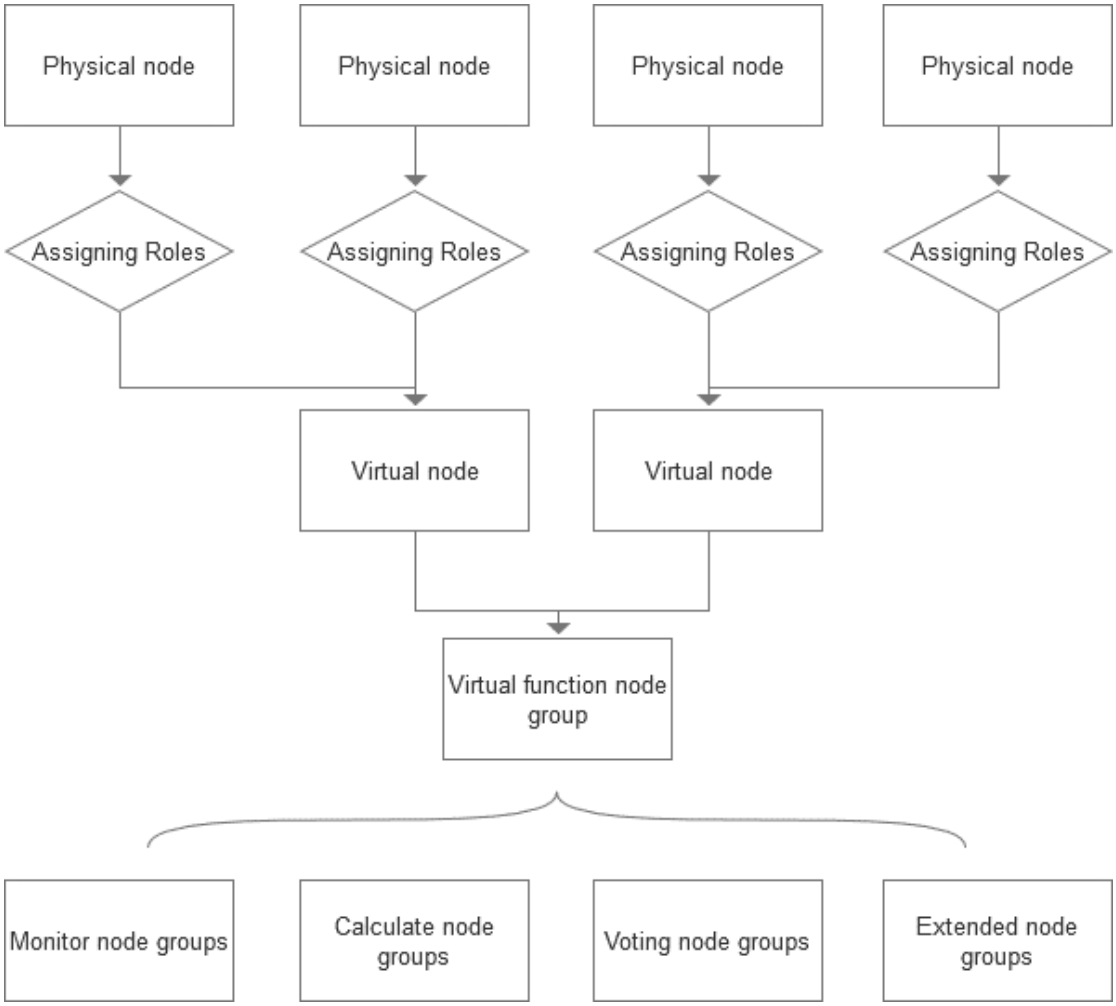
Set T as the time period parameter, and dynamically adjust the statistics to stabilize the T period after the node is stable. This ensures that the system has the length of time required for two different nodes to survive at 100% of the last period of T.For example, the calculated total node activity/trusted node ratio=M, M is constant during the last 30 minutes of the specified time point, and the same node behavior total/trusted node ratio is obtained in the last 30 minutes. N, N is a constant, and M>=N, then the length of T period is 30 minutes; after the ratio becomes smaller, the settlement length of T period is automatically extended until M>=N.

2. Judging stable nodes

Stable node calculation method:

The physical stability of a physical node refers to the need to continue to run T time, and reach the top 10% of the overall node availability. The node can adjust each T time, set the initial time period is Ts, at least X nodes become stable nodes in the Ts period. Then take the first 10% nodes as a stable node, X is the actual number of nodes in the virtual role group;

3. Node virtualization and dynamic full nodes



Node virtualization process

Assign virtual characters based on trusted stable nodes, the nodes are grouped into roles according to the network circulation capacity, computing capacity and storage capacity.
A set of role-oriented physical nodes form a virtual node, which is also an information-wide node. The actual physical nodes under the virtual node perform work assignments, and the internal information of each virtual node remains consistent and outputs work. Each virtual node is assigned its own role identities and forms a group of virtual function nodes. The last node to leave the system in each virtual node group that saves node information and is responsible for node reorganization. The role of each actual physical node is adjusted according to the control of the computing center, and it is not allowed to assume the same role of the same node group more than two consecutive times.

4. Behavior monitoring

All the behavior of each physical node is entered into the monitoring virtual node group for aggregation and output to the computing node group for analysis. The behavior of a trusted stable node still needs to be monitored and calculated periodically after completing the deduplication and identifying the credibility. When the same-role behavior difference between a node's T period and T-1 period is determined to be similar to less than 0.5, it is automatically downgraded to an untrusted node, and all role node rights are lost and recalculated.

5. Node communication ID

Each physical node only communicates with the physical nodes and other virtual nodes within the virtual node group. Since the virtual nodes are generated by the system and can be dynamically adjusted, the relative stability of each node's communication can be maintained to avoid inconsistency in information transmission.

A comparison with existing consensus voting mechanism：

Compared to the existing consensus mechanisms, POVDRG is more dependent on individuals and more like the division of labor and decentralized governance structure of human society.

Project	POW	POS	DPOS	PBFT	DAG	POVDRG
Characteristic	Encourage force	Encourage holding coin	Encourage banker	Encourage small scale	Encourage trading	Encourage stability and personalization
Risks	Machine Monopoly	Nothing-at-stake attack	Oligopoly	Inefficient operation on a large scale	Hardware device compatibility limitations	The number of participating nodes is less than the number of roles
Security	Hash encryption algorithm guarantee	Big holders guarantee	Centralized Large holder Guarantee	A sufficient proportion of honest nodes guarantee	Large number of transactions guarantee	Sufficient personal assurance

Efficiency	Limited by block speed	Limited by the performance of computing resources	Centralized efficiency	Small scale efficiency	Affected by transaction size	High efficiency central role
Extensibility	Independent node computing extension	Reduced performance after scaling	New node attaches to oligopoly	Equal role extension	Join the transaction and expand	Verification after role differentiation
Resource consumption	High computational power consumption	Big holders consume large resources	Central resource consumption	Larger consumption increases	No mining	Multi-role sharing consumption

Future Applications of POVDRG：

In the future, virtual dynamic role group voting can be applied to fields such as sociology, behavioral psychology, game theory, and network security protection on a larger scale, and reduce the consumption of a specific item. The hardware will also develop and integrate multiple features according to actual needs.