Proof of Synergy: Formal Mathematical Proof and Game Theory Analysis

D.Krizhanovskyi

September 13, 2024

1 Introduction

This document presents a formal mathematical proof and analysis of the stability of the Proof of Synergy (PoSyg) consensus algorithm. The main goal is to demonstrate the system's resilience to strategic attacks by participants using game theory and economic incentives. I begin by describing the fundamental mechanics of the PoSyg system and proceed with proofs of its stability using Nash equilibrium and coalition game theory.

2 Game-Theoretic Model of PoSyg

In the PoSyg system, each participant i has a synergy score S_i, which represents their contribution to the network's security and stability. The system allows participants to choose between two strategies:

- H_i: Honest behavior, where participants follow the network rules.
- A_i: Dishonest behavior, where participants attempt to attack the network.

The goal of each participant is to maximize their utility U_i, which depends on their synergy score S_i, earned tokens T_i, and penalties P_i imposed for dishonest behavior. The utility function is given by:

$$U_i = f(S_i, T_i, P_i)$$

where S_i is updated based on the participant's behavior over time.

3 Nash Equilibrium in PoSyg

Objective: Demonstrate that the PoSyg system has a Nash equilibrium where participants prefer honest behavior over dishonest behavior.

In PoSyg, the synergy score $S_i(t)$ of participant i evolves according to:

$$S_i(t+1) = S_i(t) + \alpha H_i(t) - \beta A_i(t)$$

where:

- $H_i(t) = 1$ if participant i behaves honestly at time t; otherwise, $H_i(t) = 0$.
- $A_i(t) = 1$ if participant i behaves dishonestly at time t; otherwise, $A_i(t) = 0$.
- α is the reward for honest behavior.
- β is the penalty for dishonest behavior.

Claim: The system achieves a Nash equilibrium when all participants behave honestly. That is, if all participants choose $H_i = 1$, no individual has an incentive to deviate by choosing $A_i = 1$.

Proof: Assume all participants are behaving honestly at time t, so for every i, $H_i(t) = 1$ and $A_i(t) = 0$. The total utility of participant i under honest behavior is:

$$U_i(H, H) = T_i(S_i) - P_i(H)$$

where $T_i(S_i)$ is the token reward as a function of synergy, and $P_i(H) = 0$ because no penalties are applied for honest behavior.

Now, consider the case where participant i deviates and chooses dishonest behavior $A_i(t) = 1$. The participant's synergy is penalized:

$$S_i(t+1) = S_i(t) - \beta$$

and they receive a penalty:

$$P_i(A) = \text{Slashing penalty} + \text{Synergy reduction}$$

Thus, their total utility becomes:

$$U_i(A, A) = T_i(S_i - \beta) - P_i(A)$$

For honest behavior to be the Nash equilibrium, I require that:

$$U_i(H, H) > U_i(A, A)$$

Substituting the expressions for $U_i(H, H)$ and $U_i(A, A)$, we get:

$$T_i(S_i) - 0 > T_i(S_i - \beta) - P_i(A)$$

Since $T_i(S_i)$ is a monotonically increasing function and $P_i(A)$ is strictly positive, the inequality holds, proving that honest behavior is the Nash equilibrium.

4 Coalition Stability and Sybil Resistance

4.1 Coalition Stability

Objective: Prove that the PoSyg system is resistant to coalition attacks by limiting the size of coalitions through penalties.

Let C denote a coalition of n participants. The total synergy of the coalition is:

$$S_C = \sum_{i \in C} S_i$$

If the coalition size n exceeds the maximum allowed size M, the coalition is penalized. The penalty is given by:

$$P_C(n) = \gamma \cdot (n - M)$$

where γ is the penalty factor for exceeding the coalition size limit.

The total utility of the coalition under coalition behavior is:

$$U_C = T_C(S_C) - P_C(n)$$

where $T_C(S_C)$ is the token reward for the entire coalition. For $n > M$, the coalition's total utility decreases as a result of the penalty $P_C(n)$.

Claim: A coalition exceeding the size limit M will earn less than a coalition that adheres to the size limit.

Proof: Consider two coalitions: one with size $n \leq M$ and another with size $n > M$. For the larger coalition, the utility is:

$$U_C(n) = T_C(S_C) - \gamma(n - M)$$

For the smaller, non-penalized coalition, the utility is:

$$U_C(M) = T_C(S_M)$$

where $S_M = \sum_{i \in C_M} S_i$ is the synergy of the coalition with size M. Since the penalty $\gamma(n - M)$ is strictly positive, the coalition with size $n > M$ has a lower utility:

$$U_C(n) < U_C(M)$$

Thus, coalitions have no incentive to exceed the size limit, proving stability against coalition attacks.

4.2 Sybil Attack Resistance

Objective: Prove that PoSyg is resistant to Sybil attacks, where an attacker creates multiple low-synergy nodes to take control of the network.

Let an attacker create k Sybil nodes, each with minimum synergy S_{min}. The total synergy of the Sybil attack is:

$$S_{\text{Sybil}} = k \cdot S_{\text{min}}$$

To participate in consensus, each node must have a minimum synergy $S_{\text{threshold}}$. If $S_{\text{min}} < S_{\text{threshold}}$, Sybil nodes cannot participate, and the attack fails.

Proof: If $S_{\text{min}} < S_{\text{threshold}}$, then:

$$S_{\text{Sybil}} = k \cdot S_{\text{min}} < S_{\text{threshold}}$$

Since the Sybil nodes do not meet the minimum synergy requirement, they are excluded from consensus. Therefore, the attack is unsuccessful, proving Sybil resistance.

5 Conclusion

The Proof of Synergy consensus algorithm is mathematically proven to be stable against strategic attacks. Honest behavior is incentivized through a Nash equilibrium, and the system is resistant to coalition-based and Sybil attacks through penalties and synergy thresholds.