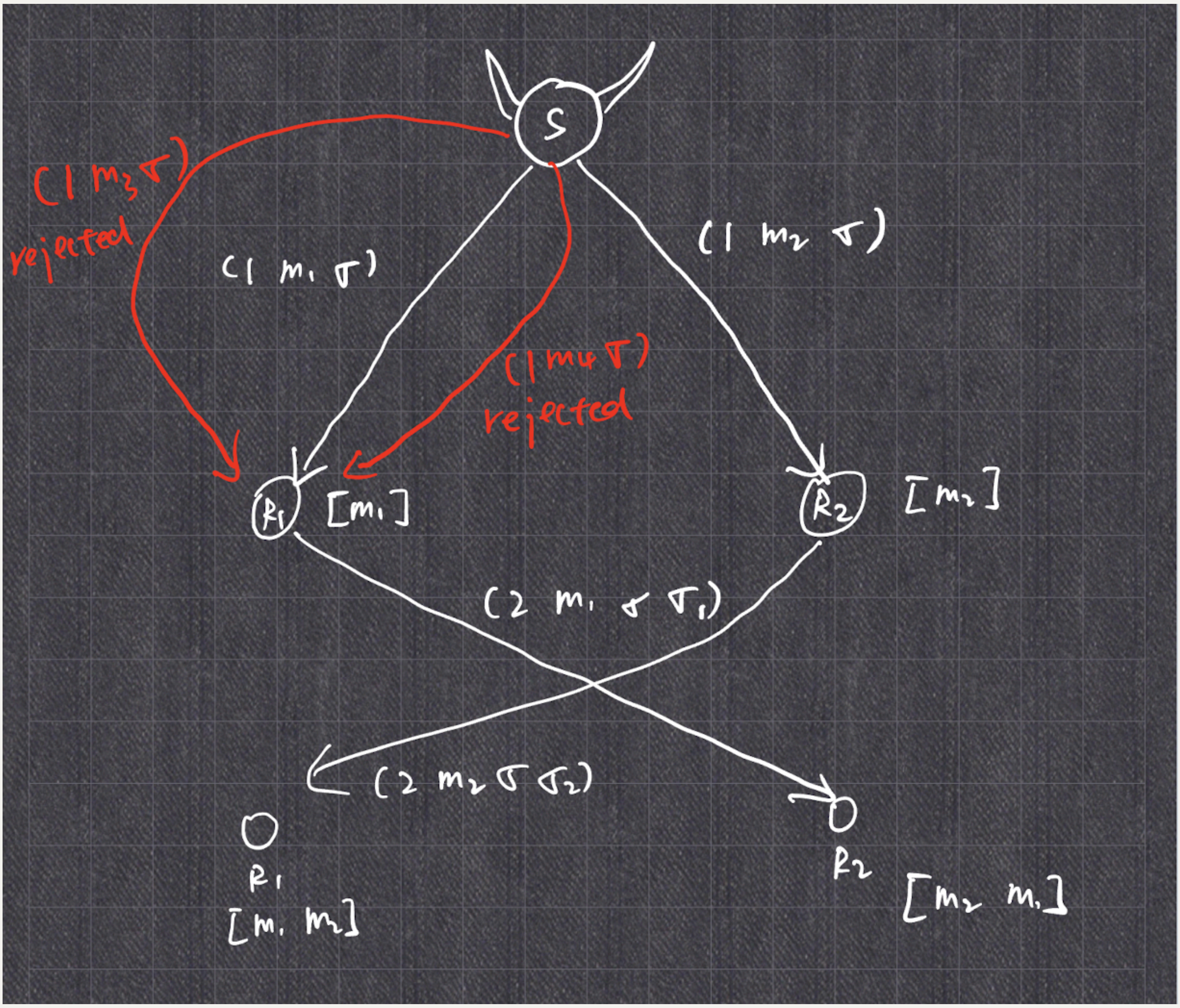
Assume we have one Byzantine-corrupted sender and two honest parties. The sender can send many different messages with the same broadcast ID within one round.

In our protocol, the node only keeps the first message with the same bid and signature in one round. If the sender sends 2 messages (1,m1,σ), (1,m2,σ) to P1, P1 will simply drop the second message(1,m2,σ). The rest part of the protocol is the same as the Dolev-Strong protocol.


S
(1 m3 σ)
rejected
(1 m1 σ)
(1 m2 σ)
(1 m4 σ)
rejected
R1
[m1]
R2
[m2]
(2 m1 σ σ1)
(2 m2 σ σ2)
R1
[m1 m2]
R2
[m2 m1]