What if a malicious user performs a Sybil attack of verification (not mining) - spawning a large number of non-mining nodes that verify and approve malicious transactions within a shard.

It does not cost much to create a lot of non-mining nodes, and if the number is huge enough it is very likely that a shard is full of them.