Assignment 3 - Understanding Attacks and Defenses

Max Liu

January 31, 2019

Bad nodes implementation

Bad nodes should only communicate with other peer bad nodes to reach a consensus and good nodes should only communicate with other peer good nodes to reach a consensus. The given implementation is correct because we first query to see if a peer has the same "goodness" status as us and if they do then we add their chain to our list of chains to feed into our consensus algorithm.

Simulate Attack

Two nodes that are peers and do not have the latest transaction in their chains are flipped to be bad nodes and mine independently. I chose nodes 1 and 8, the actions are displayed below for reference.

```
book.set_book([
                {'type':Action.NEW_TX,'n1':'node0','n2':'node8'},
                {'type':Action.MINE,'n1':'node3'},
                {'type':Action.RESOLVE_ALL},
                {'type':Action.NEW_TX,'n1':'node3','n2':'node7'},
                {'type':Action.MINE,'n1':'node7'},
                {'type':Action.RESOLVE_NODES, 'nodes':['node0', 'node3', 'node4', 'node5', 'node6']},
                # max's attack with flipped nodes 1 and 8
                {'type': Action.FLIP, 'n1': 'node1'}, # flipped node1
                {'type': Action.FLIP, 'n1': 'node8'}, # flipped node8
                {'type':Action.MINE,'n1': 'node1'},
                {'type':Action.RESOLVE_NODES, 'nodes': ['node1', 'node8']},
                {'type':Action.MINE,'n1': 'node1'},
                {'type':Action.RESOLVE_NODES, 'nodes': ['node1', 'node8']},
                {'type':Action.MINE,'n1': 'node1'},
                {'type':Action.RESOLVE_NODES, 'nodes': ['node1', 'node8']},
                {'type':Action.MINE,'n1': 'node1'},
                {'type':Action.RESOLVE_NODES, 'nodes': ['node1', 'node8']},
                {'type': Action.FLIP, 'n1': 'node1'},
                {'type': Action.FLIP, 'n1': 'node8'},
                {'type':Action.MINE,'n1':'node3'},
                {'type':Action.RESOLVE_ALL},
            ])
```

Consensus Update

The original consensus algorithm allowed for this type of attack because it only cares if 2 nodes share a common prefix so 2 bad nodes that are very powerful can mine ahead of the good chain and cause all of the nodes to switch over to the bad chain.

In order to protect against this malicious attack, I have changed the consensus algorithm so that a node will only reach a consensus on a chain if a **majority** of the chains share a common prefix. This prevents a small number of bad nodes from forcing the rest of the network to switch over. However, in this assignment if the bad nodes do not have sufficient good nodes as its peer, it will not resolve back to the good chain.

Reflections

Question 1

This attack is technically possible in the Bitcoin blockchain but is unlikely unless a group of bad nodes control over 51% of the computing power. Bitcoin selects the longest chain as the true chain and currently uses a very computationally expensive POW. It would be very difficult for bad nodes to mine blocks at a rate faster than the good nodes and switch the chain over to the bad chain. As mentioned before, this would require the bad nodes to have a majority of the computing power in the network.

Question 3

Because the consensus algorithm is now looking for a majority of the chains to share a common prefix, this can lead to an attack where many bad nodes work together to create a network with a lot of connections. When new nodes join the network they can be sucked into this bad node network if a majority of its peers are bad nodes. This network is also still prone to a 51% attack. If the computing power of the bad nodes exceeds 51% and they have a large network that can propagate the bad chain, the entire blockchain will eventually switch over to the bad chain.