ECE 598PV Principles of Blockchains Assignment 4

Date Assigned: April 16, 2020
Date Due: April 23, 2020

Abstract. We abstract the underlying P2P network by supposing that any transmit packet reaches all participating nodes within delay Δ. This network delay in conjunction with the mining rate of blocks leads to *forking*: honest nodes do not have the latest view of the blocktree and could be mining on a block that is no longer the tip of the longest chain in the latest blockchain. The actions of the adversary exacerbates the forking and the larger the network delay (for a given mining rate), the more successful double-spend attacks are. In this assignment we explore some attacks the adversary can mount and how their success interacts with the network delay and mining rate.

Model. We consider the following network model: any block transmit on the network reaches every other node in time less than or equal to Δ (seconds). The adversary controls the network enough so that: (a) it receives any honest node's transmission instantly; (b) can deliver the packet to any participating honest network node at any time of its choosing, as long as the delivery time is within Δ from the time of transmission (different honest nodes may thus receive the block at different times). We suppose that there are a larger number of honest nodes, each with a very small fraction of the total mining power, so the chance that the same node succeeding in mining successive blocks is negligible.

Questions.

1. In this exercise we study a specific adversary delivery strategy: delay any honest node's transmission by exactly Δ seconds and deliver at the same time to all honest nodes. This way, all honest nodes have the same view of the blocktree. Honest nodes follow the longest chain protocol: they mine on the tip of the longest chain in their blocktree. If there is more than one longest chain, then we consider two scenarios: (A) – all honest nodes pick the same one of the longest chains and mine on its' tip; (B) – the honest nodes are split and mine on the tip of each of the longest chains with equal mining power. In scenario (A), the honest mining succeeds at a random time exponentially distributed with mean $\frac{1}{f(1-\beta)}$. In scenario (B), the honest mining in any one of the longest chains succeeds at a random time exponentially distributed with mean $\frac{\ell}{f(1-\beta)}$, where ℓ is the number of longest chains. The adversary uses its hash power to mine a *private chain* (from Genesis). The adversary succeeds in its mining effort at a random time, exponentially distributed with mean $\frac{1}{f\beta}$. The adversary is successful in a private attack if **it's privately held chain of blocks is no shorter than the honest chain and the honest chain is longer than a parameter** k. Create an event-driven simulation testbed with two parties: one adversary and the other honest, following the strategy described above.

   (a) Plot the probability of success of the private attack for different values of β, f, Δ, k. Is your plot the same or different for scenarios (A) and (B)? Observe that for some conditions on β, f, Δ the success probability decays to zero as k grows large and for other conditions the success probability is always 1.

   (b) You should be able to empirically observe that the probability of success of the attack depends on f and Δ only on the *product* $f\Delta$. Prove mathematically that the probability of success of the private attack depends only on $\beta, f\Delta, k$.

(c) In a two dimensional plot (with one dimension representing β and the other $f\Delta$), shade the largest region you can find such that the probability of success of the private attack decreases to 0 as k grows large.

2. In this exercise we study a different adversary delivery strategy: delay any honest node's transmission such that the honest nodes all receive the packet at *exactly an integer multiple* of Δ seconds (e.g., a block mined in the time interval $[2\Delta, 3\Delta)$ will be received by all honest nodes at time 3Δ). The effect of this strategy is to create a *round-by-round* discrete-time synchronous model. Redo the three exercises from the previous question. Which adversary delivery strategy leads to more success probability: deliver after the full delay Δ or deliver at the earliest integer multiple of Δ?

3. In this exercise we study the general adversary delivery strategy. Now each honest party always works on the first longest chain it received. A *balance attack* is the following, where there will be just two public chains in the blocktree forked from Genesis:

   - If the two public chains are of unequal length, then the adversary always mines on the shorter of the two chains; the honest party mines on the longer of the two chains (following the longest chain protocol).
   - If both the public chains are of equal length, then the adversary stops mining and forces the honest party to split equally on the two public chains. Once the honest party succeeds in mining first on chain 1 (or chain 2) at time t, then the adversary starts to mine on chain 2 (or chain 1) together with the other half of honest parties. If one block is mined on chain 2 (or chain 1) before time $t + \Delta$, then the two public chains will be re-balanced by the adversary at time $t + \Delta$, otherwise the chains are of unequal length and we return to the previous step.

   We say this attack is successful if **there exists a point of time where both public chains are of equal length greater than k.** Redo the three exercises from question 1 and compare the balance attacks with private attack in question 1.

4. **Bonus**. The following is a conjectured optimal strategy. Prove or disprove.

   Starting from the genesis, the adversary mines a private chain. Meanwhile the adversary tries to split the honest nodes to work on two public chains forked from genesis with equal length by properly delivering messages. Suppose the first honest block of height 1 is mined at time t_1, and if another honest block is mined at time $t_1 + \Delta$, then the adversary delivers these two block at time $t_1 + \Delta$ and makes honest nodes split equally on these two honest blocks. We call these two public chains chain 1 and chain 2. Once the honest party succeeds in mining first on chain 1 (or chain 2) at time t_2, then if one block is mined on chain 2 (or chain 1) before time $t_2 + \Delta$, then the two public chains can be re-balanced by the adversary at time $t_2 + \Delta$. Otherwise chain 1 and chain 2 are of unequal length, the adversary should just stop balancing and use the delivery strategy in question 1.

   The adversary is successful in a private attack if **1) it's privately held chain of blocks is no shorter than the honest chain and the honest chain is longer than a parameter k; or 2) there exists a point of time where both public chains are of equal length greater than k** .

   Remark: Without success condition 2), the conjectured optimal strategy has exactly the same performance as the private attack in question 1 as splitting the honest nodes does not hurt

the growth of honest chain. And also for large k, the conjectured optimal strategy should have similar performance as the private attack in question 1 as splitting won't last for long time.