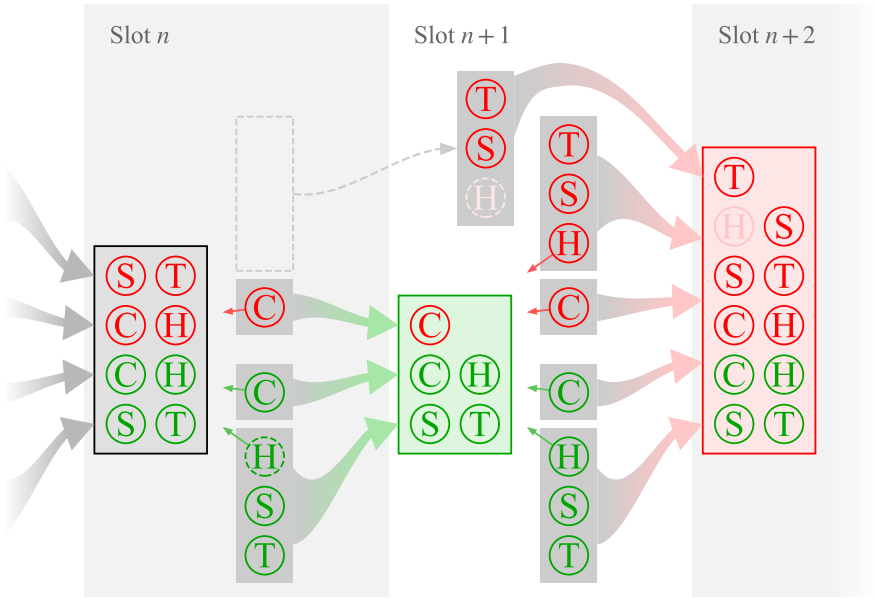

Figure 5. A discouragement attack based on withheld attestations, denying a block proposer rewards. An attacker withholds its attestations in slot n, releasing them in time for inclusion by its own block proposer in slot $n+2$, thus depriving the block proposer in slot $n+1$ of proposer rewards. As a result of the delay, the head votes will not incur rewards (faded "H") and reward reduction be applied at slot n for all head votes (dashed circle).

4.1 Withheld attestations under normal operations

The attacker may withhold its attestations under normal operations in order to deprive the others of the proposer's share of the attestation rewards, releasing the attestations just before being assigned to propose a block. To have any prospect of being profitable, the withheld attestations must be included before they accrue penalties for an untimely source vote. The requirement is thus that the attacker is assigned as a block proposer within 2-5 slots and withholds the attestation until right before proposing. Figure 5 shows the attacker withholding its attestations in slot n and releasing them in time for inclusion in its own block at slot $n+2$. The attacker will gain the block proposers' rewards for a timely source and target vote and lose out on attester rewards for the head votes. The attacker's change in rewards, relative to one base reward is thus

$$\frac{14+26}{64\times 7}a-\frac{14}{64}a=\frac{40-98}{64\times 7}a=-\frac{29a}{32\times 7}. \tag{39}$$

The others will lose out on the proposers' share of the head, source and target votes in the attestations that the attacker withholds, equaling a change of

$$-\frac{(14+14+26)a}{64\times 7}. \tag{40}$$

In addition, the reward reduction when a head attestations are missing means that the others' reward for their $1-a$ head attestations are reduced by

$$(1-a)a=a-a^2 \tag{41}$$

as well. The change in rewards for this part is therefore

$$-\frac{14(a-a^2)}{64} \tag{42}$$

The others' total change in rewards, relative to one base reward, is thus

$$-\frac{(14+14+26)a}{64\times 7}-\frac{14(a-a^2)}{64}=\frac{49a^2-76a}{32\times 7}. \tag{43}$$

The griefing factor G_W for the withheld attestation attack is computed from Eq. 39 and Eq. 43 as

$$G_W=\frac{(49a^2-76a)/(32\times 7)}{-29a/(32\times 7)}\approx 2.62-1.69a. \tag{44}$$