1 Evidence of theory for our countermeasure.

Next, we will demonstrate how many onion services the attacker needs to create in order to ensure that r onion services are successfully accepted by the target HSDir.

We aim to compute the cost that HSDirSniper must spend to generate r malicious onion services to attack an HSDir, i.e., the attacker needs to generate at least k onion services to ensure that the descriptors of the r onion services will not be filtered by the target HSDir. For simplicity, we assume that the DHT consists of N HSDirs and the index interval d_i (see line 312 in the manuscript) between HSDir is equal. According to the rules we set for filtering descriptors, the probability p that an $HSDir_i$ receives a randomly generated onion service's descriptor is:

$$p = 8 * 1/N = 8/N, \tag{1}$$

where N denotes the number of all HSDirs.

Since the selection of an HSDir by an onion service is an independent event, the above process can be interpreted as k fold independent Bernoulli trials that generate onion services, where at least r onion services can be received by the target HSDir. Let $Pr(k, r, p)$ denote the probability mass function of the above Bernoulli trials, which follows a binomial distribution:

$$Pr(k, r, p) = \binom{k-1}{r-1} p^r * (1-p)^{k-r} \tag{2}$$

Then the expected number of experiments $E(k)$ can be calculated by

$$\begin{aligned} E(k) &= \sum_{k=1}^{\infty} k * Pr(k, r, p) \\ &= \sum_{k=1}^{\infty} k * \binom{k-1}{r-1} p^r * (1-p)^{k-r} = \frac{r}{p}, \end{aligned} \tag{3}$$

where r represents the number of onion services will not be filtered by the target HSDir.

We randomly selected a day's consensus file (e.g., 2023-06-10 12:00:00) to construct the DHT, where the length of DHT was 4003, i.e., $N = 4003$. Taking it into Eq.(1), we get $p \approx 0.002$. Finally, substituting p into Eq.(3), we obtain the relationship between expected number $E(k)$ of onion services generated by the attacker and the number r of onion services that can be received by the target HSDir: $E(k) = 500 * r$.