A Proof for the bound of $P_{m=1}^{detect,diff}$

When we assume that a centralized RNG generates redundant computations for a layer l, we assume we generate R_l redundant computations that do not overlap. Then, the probability that one base computation in layer l device i does not have a redundant copy is $1 - r_{l,i}$, assuming each device in layer l computes the same number of base and redundant computations.

The probability of detecting a single maliciously attacked device is: $P_{m=1}^{detect,cen} = 1 - (1 - r_{l,i})^n$.

The comparison between the probability of detection for centralized RNG and independent RNG methods is limited to the situation that only one device is attacked, as this is the only secure application scenario for the centralized RNG method. In particular, we assume the worst case is that the attacker targets $n = 1$ base computation.

The expected amount of inferences E to successfully detect the attack and the number of inferences F to detect the attack when the confidence is $c\%$ can be calculated in the same way as stated in Section 3.4 in our paper **An Efficient Distributed Machine Learning Inference Framework with Byzantine Fault Detection**.

For simplicity, in this appendix we denote the redundancy overhead $r_{l,i}$ as r, and the number of devices N_l as N. $r \in (0, 1)$, $N \in [2, +\infty)$, $N \in Z$

$$\begin{aligned} P_{m=1}^{detect,diff} &= P_{m=1}^{detect,cen} - P_{m=1}^{detect,ind} \\ &= r - 1 + (1 - \frac{r}{N-1})^{(N-1)} \end{aligned} \tag{1}$$

Assume $x = N - 1$, then $x \in [1, +\infty)$, $x \in Z$, then:

$$P_{m=1}^{detect,diff} = r - 1 + (1 - \frac{r}{x})^x \tag{2}$$

Assume $g(x, r) = r - 1 + (1 - \frac{r}{x})^x$, $f(x, r) = (1 - \frac{r}{x})^x$. Because $\frac{r}{x} \in (0, 1)$, then $1 - \frac{r}{x} \in (0, 1)$, therefore $f(x, r) = (1 - \frac{r}{x})^x \in (0, 1)$.

$\ln f(x, r) = x \ \ln(1 - \frac{r}{x})$

Derive both sides of equations with x:

$$\begin{aligned} \frac{\frac{df(x,r)}{dx}}{f(x,r)} &= \ln(1 - \frac{r}{x}) + x \ \frac{r}{x^2} \frac{1}{1 - \frac{r}{x}} \\ &= \ln(1 - \frac{r}{x}) + \frac{r}{x - r} \end{aligned} \tag{3}$$

$$\frac{df(x,r)}{dx} = f(x,r) \left(\ln(1 - \frac{r}{x}) + \frac{r}{x - r} \right) \tag{4}$$

Assume $h(x, r) = \ln(1 - \frac{r}{x}) + \frac{r}{x-r}$

$$\begin{aligned} \frac{dh(x,r)}{dx} &= \frac{1}{1 - \frac{r}{x}}(-1)(-\frac{r}{x^2}) - \frac{r}{(x-r)^2} \\ &= \frac{-r^2}{x(x-r)^2} \end{aligned} \tag{5}$$

Clearly, $\frac{dh(x,r)}{dx} < 0$, this indicates $h(x, r)$ monotonically decreas with the increase of x, when $x \in [1, +\infty)$, $x \in Z$. Therefore, we know:

$$\begin{aligned} h(x,r)_{min} &= h(x,r)_{x \to +\infty} \\ &= \ln(1^-) + 0^+ \\ &= 0 \end{aligned} \tag{6}$$

Thus $h(x, r) > 0$ is always true when $x \in [1, +\infty)$, $x \in Z$, and $r \in (0, 1)$.

From Eq. 4:

$$\frac{df(x,r)}{dx} = f(x,r) \cdot h(x,r) \tag{7}$$

As it is proven that $h(x,r) > 0$, $f(x,r) = (1-\frac{r}{x})^x \in (0,1) > 0$ in the given range of x and r, then we have $\frac{df(x,r)}{dx} > 0$. This proves that $f(x,r)$ monotonically increases with the increase of x. The upper bound of $f(x,r)$ should be:

$$\begin{aligned} f(x,r)_{max} &= f(x,r)_{x\to+\infty} \\ &= (1-\frac{r}{x})^x_{x\to+\infty} \end{aligned} \tag{8}$$

According to the definition of e, $e^k = \lim_{n\to+\infty}(1+\frac{k}{n})^n$, then $f(x,r)_{max} = e^{-r}$. From here, we can conclude that:

$$\begin{aligned} P_{m=1}^{detect,diff} = g(x,r) &= r - 1 + (1-\frac{r}{x})^x \\ &= r - 1 + f(x,r) \\ &< r - 1 + e^{-r} \end{aligned} \tag{9}$$

Conclusion:

The detection probability differences $P_{m=1}^{detect,diff}$ between the centralized RNG $P_{m=1}^{detect,cen}$ and independent RNG $P_{m=1}^{detect,ind}$ methods has an upper bound of $r_{l,i} - 1 + e^{-r_{l,i}}$.

To find out the trend of $g(x,r)_{max}$ according to the change of r, we derive $g(x,r)$ with r:

$$\begin{aligned} g(x,r)_{max} &= r - 1 + e^{-r} \\ \frac{dg(x,r)_{max}}{dr} &= 1 - e^{-r} \in (0, 1-\frac{1}{e}) > 0 \end{aligned} \tag{10}$$

This shows that $g(x,r)_{max}$ increases monotonically with the increase of r. The largest possible value of $P_{m=1}^{detect,diff}$ is $g(x,r)_{max}(r = 1^-) = \frac{1}{e} \approx 0.368$. When $r = 10\%$, the upper bound of $P_{m=1}^{detect,diff}$ is around 0.005, and when $r = 20\%$, the upper bound of $P_{m=1}^{detect,diff}$ is around 0.019.

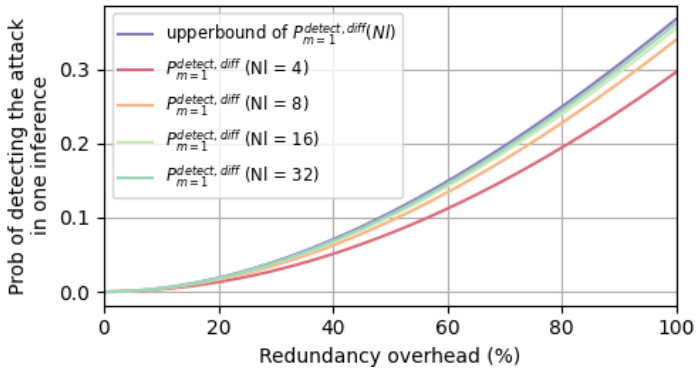

Figure 1: The variation of $P_{m=1}^{detect,diff}$ and its maximum theoretical limit with changing redundancy overhead.