PROOF

For TFIPA, we derive the range for the number of malicious users and the conditions for the existence of a solution to the ILP problem, supported by detailed proofs. For TFIPA+, we establish the upper bound on the attack success rate and present its derivation. Similar analytical approaches can be applied to TFOPA and TFOPA+.

1 The range of the number of malicious users u.

In Section 5.1 of the paper, we use the Gurobi optimizer to solve the ILP problem. we derive feasible parameter ranges to ensure the existence of a valid solution. For the case where $\boxtimes_j =$ " $\geq$ ", the minimum number of malicious users u must satisfy $u \in [max(2, \max_j \frac{t_j \cdot \tilde{n} - \tilde{C}^n_{v_j}}{1-t_j}), +\infty)$. Proof is as follows.

Combining constraints $\tilde{C}^u_{v_j} \geq t_j \cdot (\tilde{n} + u) - \tilde{C}^n_{v_j}$ and $0 \leq \tilde{C}^u_{v_j} \leq u$ yields:

$$t_j \cdot (\tilde{n} + u) - \tilde{C}^n_{v_j} \leq u,$$

By transferring items, we obtain:

$$(t_j - 1) \cdot u \leq \tilde{C}^n_{v_j} - t_j \cdot \tilde{n}.$$

Because of $0 < t_j < 1$, $t_j - 1 < 0$, inequality direction reversal:

$$u \geq \frac{t_j \cdot \tilde{n} - \tilde{C}^n_{v_j}}{1 - t_j}.$$

At the same time, $u \geq 1$, therefore:

$$u \geq max(1, \max_j \frac{t_j \cdot \tilde{n} - \tilde{C}^n_{v_j}}{1 - t_j}).$$

We can obtain the range of u: $u \in [max(1, \max_j \frac{t_j \cdot \tilde{n} - \tilde{C}^n_{v_j}}{1-t_j}), +\infty)$.

2 The parameter range of the solution exists.

In Section 5.1 of the paper, for the case where $\boxtimes_j =$ " $\geq$ ", to ensure the existence of a solution for u, it is necessary to satisfy:

- $\frac{t_j \cdot \tilde{n} - \tilde{C}^n_{v_j}}{1-t_j}$ is a finite real number.
- $\tilde{C}^u_{v_j} \geq 1$ must be established.

We can obtain $t_j \cdot (\tilde{n} + u) - \tilde{C}^n_{v_j} \geq 1$. By substituting $u \geq \frac{t_j \cdot \tilde{n} - \tilde{C}^n_{v_j}}{1-t_j}$, we obtain:

$$\frac{1 + \tilde{C}^n_{v_j}}{1 + \tilde{n}} \leq t_j < 1.$$

Therefore, we can conclude that the condition for the existence of a solution is $\frac{1+\tilde{C}^n_{v_j}}{1+\tilde{n}} \leq t_j < 1$.

3 The upper limit of attack success rate α.

In Section 5.2 of the paper, we have $t_j' = t_j + \Delta f_{v_j}$, $t_j \geq \frac{1+\tilde{C}_{v_j}^n}{1+\tilde{n}}$, and $\Delta f_{v_j} \geq \sqrt{\frac{\mathbb{D}(\hat{f}_{v_j})}{2(1-\alpha)}}$, and by substituting them, we can obtain the inequality:

$$t_j' \geq \frac{1+\tilde{C}_{v_j}^n}{1+\tilde{n}} + \sqrt{\frac{\mathbb{D}\left(\hat{f}_{v_j}\right)}{2(1-\alpha)}}.$$

t_j' has a constraint condition: $t_j' < 1$, we can obtain the inequality:

$$\frac{1+\tilde{C}_{v_j}^n}{1+\tilde{n}} + \sqrt{\frac{\mathbb{D}\left(\hat{f}_{v_j}\right)}{2(1-\alpha)}} < 1.$$

Through simplification, we can obtain a constraint on the attack success rate α:

$$\alpha < 1 - \frac{\mathbb{D}\left(\hat{f}_{v_j}\right)(\tilde{n}+1)^2}{2(\tilde{n}-\tilde{C}_{v_j}^n)^2}.$$