

CDNにおける遺伝子アルゴリズムを使用して 最適なキャッシュ汚染攻撃

1. はじめに

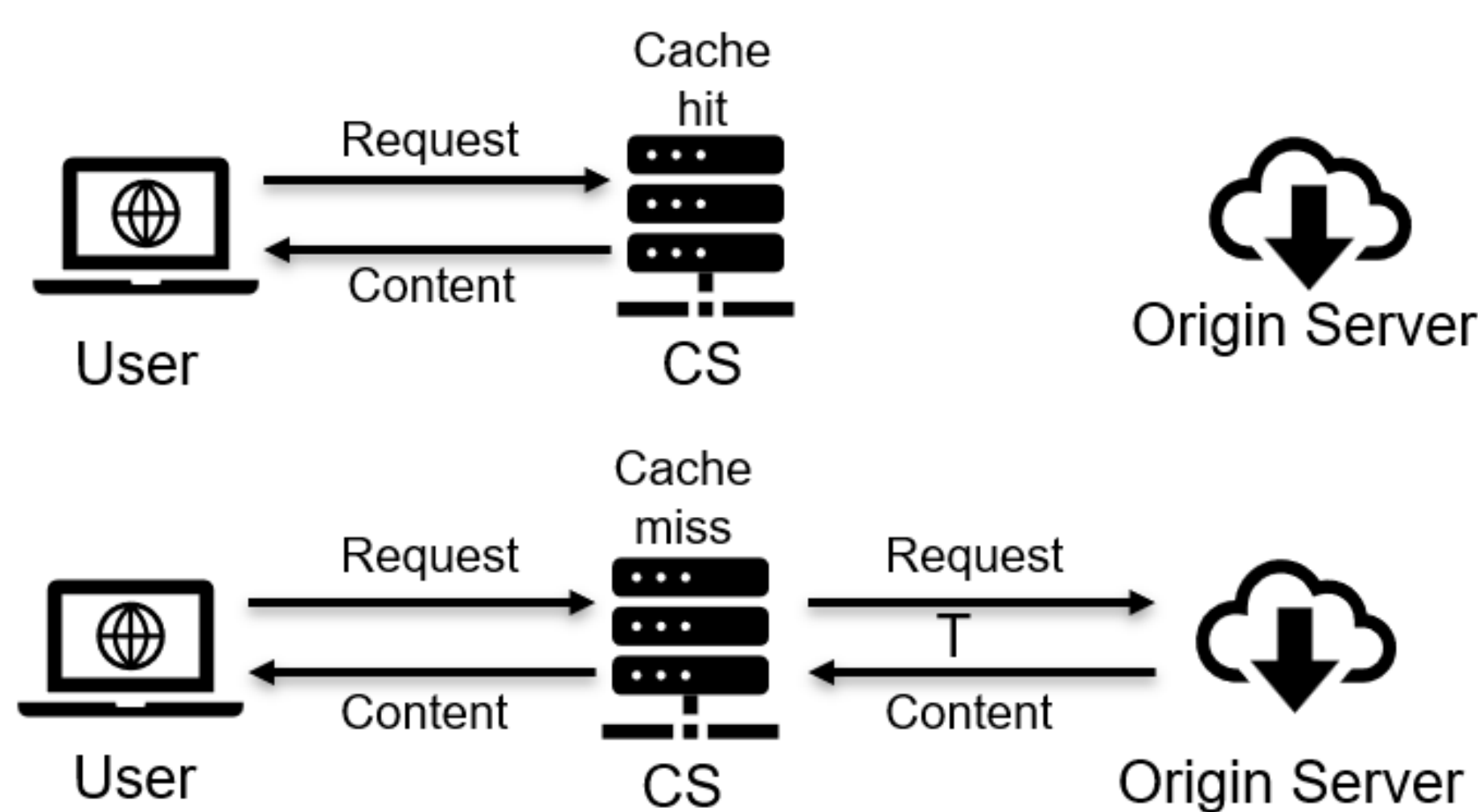
- CDNの普及により、CDNに対する攻撃はますます注目を集めている
- 攻撃者の視点から分析することは珍しい



遺伝子アルゴリズムを使用して攻撃戦略を最適化

2. Content Delivery Network

- ユーザが要求をキャッシュサーバ（CS）に送信
 - キャッシュヒットが発生すると、CSはコンテンツをユーザに送信
 - キャッシュミスが発生した場合、CSはリクエストをオリジンサーバに送信し、オリジンサーバはコンテンツをCSに送信し、それはキャッシュされ、ユーザに送信



3. 分析モデル

- M/M/1 キューでは、CDNのパフォーマンスを評価するために平均応答時間Wを使用

$$W = \frac{1}{\mu - \sum_{i=1}^M \lambda_i}$$

- Che 近似を通じて、コンテンツのキャッシュヒット比をその人気と関連付ける

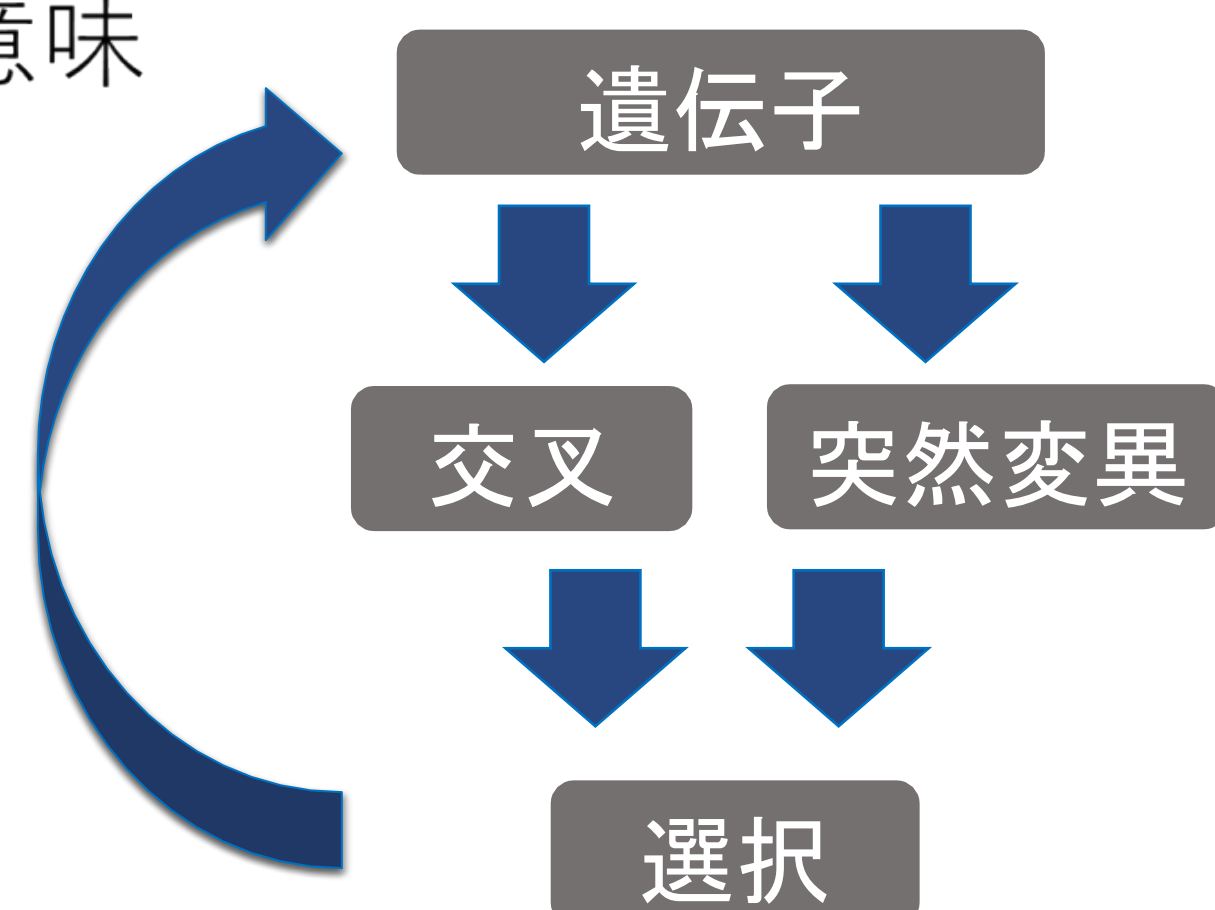
$$h_i \approx 1 - e^{-q_i t_c}$$

$$\sum_{i=1}^M h_i = C$$

4. 遺伝的アルゴリズム

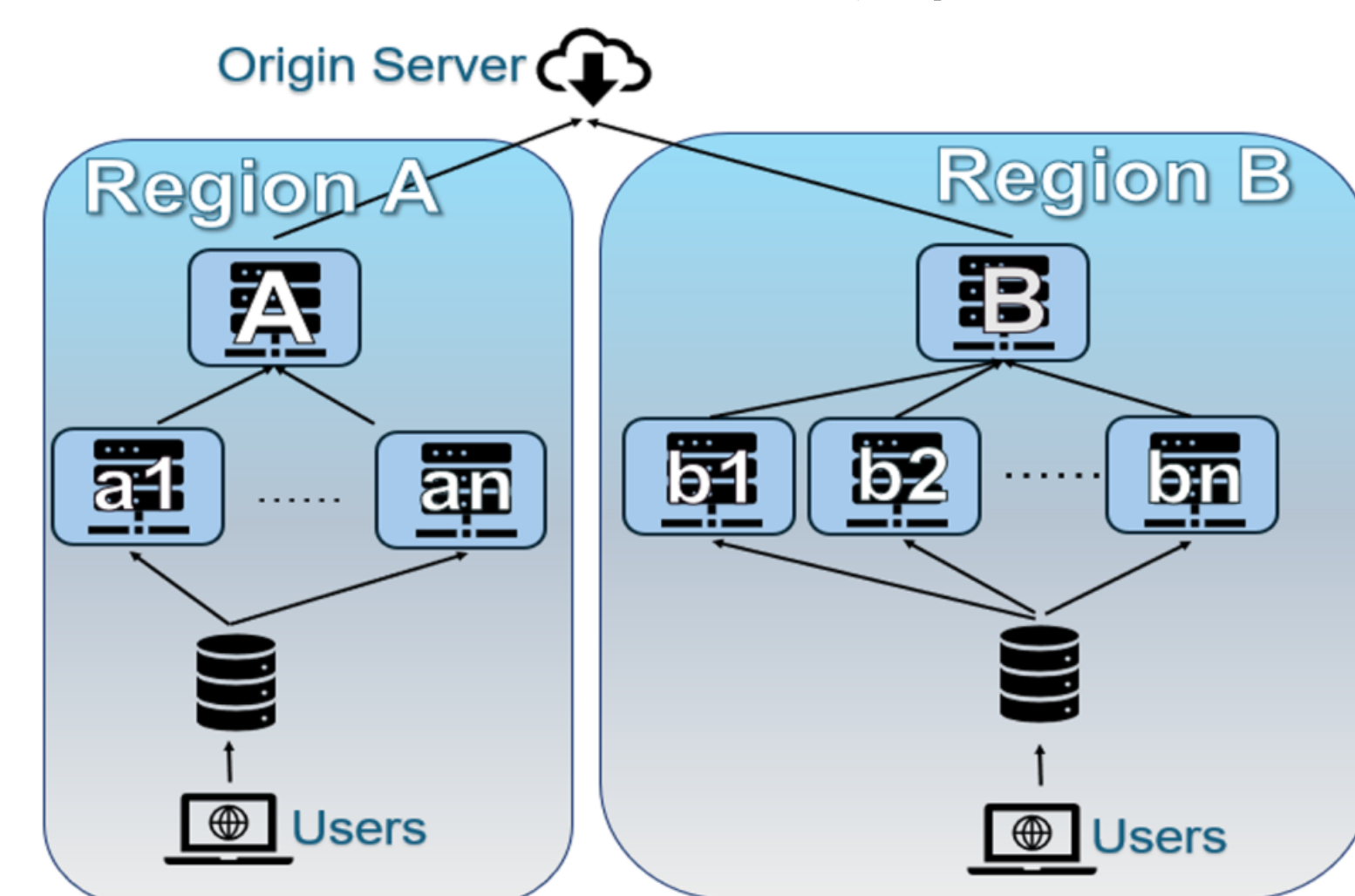
- 遺伝的アルゴリズム（GA）は、突然変異、交叉、選択などの生物学的にインスピレーションされた演算子に頼って最適化のための高品質のソリューションを生成するために使用される
- S_n^i 遺伝子として、攻撃者がサーバ n のコンテンツ i に送信するリクエストの割合を意味

- 攻撃後の平均応答時間をフィットネスとして選択操作を行う



5. CDNモデル

- CDNモデルは、複数の層でCSを持つ複数の地域で構成されています。
- オリジンサーバは5つ地域にコンテンツコピーを提供
- 中央サーバは、元サーバからコンテンツを保存し、エッジサーバに送信するための大きなキャッシュサイズを持っている
- エッジサーバは、小さなキャッシュサイズで人気のあるコンテンツを迅速に提供。



- 地域Aにおける平均応答時間

$$\begin{aligned} r_e^A &= W_a & -a_n \text{にキャッシュヒット} \\ r_c^A &= W_a + W_A + T_1 & -A \text{にキャッシュヒット} \\ r_o^A &= W_a + W_A + W_o + T_1 + T_2 & -A \text{と } a_n \text{にキャッシュミス} \end{aligned}$$

- 地域Aにおけるコンテンツiの平均応答時間

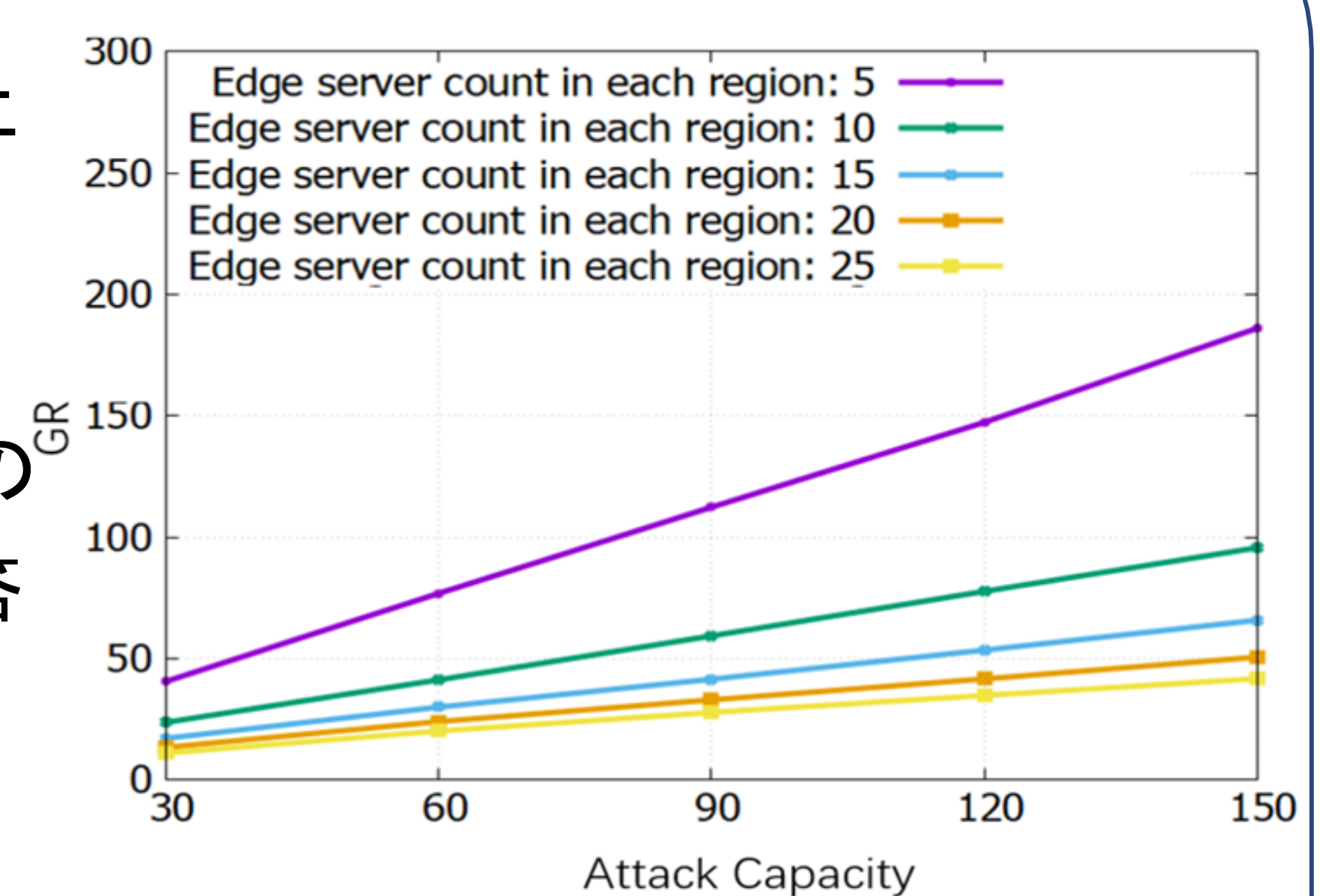
$$R_i^A = h_i^{an} r_e^A + (1 - h_i^{an}) h_i^A r_c^A + (1 - h_i^{an})(1 - h_i^A) r_o^A$$

- 地域Aのすべてのリクエストの平均応答時間

$$R_A = \sum_{i=1}^M \frac{\lambda_i^A R_i^A}{\sum_{i=1}^M \lambda_i^A}$$

6. 評価

- 各コンテンツにリクエスト率をzipf法に基づいて設定
- 平均応答時間（GR）の成長率を使用して応答時間の変化を示す



- 同じ攻撃容量で、エッジサーバ数が少ない地域は攻撃にもっと脆弱
- 攻撃容量が増加するにつれて、エッジサーバ数が少ない地域におけるGRの成長率が増加

Paramater	Value
Number of contents provided, M	100
Edge servers' cache size	20
Central servers' cache size	50
Zipf law parameter	4
Edge server number in target area	5
Requests rate to each edge server, λ	30 /second
Av. service time of Edge servers, $1/\mu_1$	10 ms
Av. service time of Central servers, $1/\mu_2$	2 ms
Av. service time of origin server, $1/\mu_o$	1 ms
Latency, T_1	500 ms
Latency, T_2	300 ms