MEC に対するキャッシュポリューション攻撃の影響分析

Investigating Effect of Cache Pollution Attack at MEC Cache

芦原 大和　　上山 憲昭
Takakazu Ashihara　　Noriaki Kamiyama
福岡大学 工学部 電子情報工学科
Faculty of Engineering, Fukuoka University

1. はじめに

バックホールのトラヒック負荷を低減することで Web 閲覧や動画配信サービスを快適に行うため，5G セルラーネットワークの基地局にキャッシュサーバを設置する Mobile Edge Computing (MEC) が精力的に検討されている．しかし悪意を持ったユーザが意図的に低人気のコンテンツに多数の要求を行うことで低人気コンテンツをキャッシュさせ，キャッシュの効果を低下させるキャッシュポリューション攻撃 (CPA: cache pollution attack) の問題が指摘されている [1][2]．しかし CPA ホスト数や CPA 対象コンテンツ数などの各種パラメータが CPA の効果に与える影響は分析されていない．そこで本稿では，各種パラメータが CPA のキャッシュヒット率低下効果に与える影響を計算機シミュレーションにより評価する．

2. キャッシュポリューション攻撃 (CPA)

CPA には，Locality-disruption 型と False-locality 型の 2 種類の攻撃法が存在する．一般にキャッシュの性能はコンテンツの人気の偏りが強いほど大きくなるため，Locality-disruption 型の CPA では，攻撃ホストは全てのコンテンツに対して一様に要求を発生させ，コンテンツの人気の偏りを緩やかにすることでキャッシュの効果を低下させる．一方 False-locality 型の CPA では，攻撃ホストは低人気のコンテンツに対して多数の要求を発生させコンテンツの人気の順位を入れ替えることで，正常ユーザの配信要求に対するキャッシュヒット率を低下させる．本稿では，両方のタイプの CPA を想定する．

3. CPA による影響の評価

$M = 10,000$ 個のコンテンツに対し，人気の高いものから順に $1, 2, \cdots, M$ のラベリングがされていることを想定する．キャッシュ置換方式としては，最後に要求されてからの経過時間が最大のコンテンツを削除する LRU (least recently used) を想定する．特に断らない限り，キャッシュサイズ B を 500 に，正常ホスト数 N を 10,000 に，CPA ホスト数 N_c を 10 に，正常ホストからの総要求発生レートに対する CPA ホストからの総要求発生レートの比率 β を 1 に，CPA 対象コンテンツ数 C を 500 に設定する．CPA ホストはコンテンツの人気順位を知っていることを想定し，最も低人気のコンテンツ M から C 個のコンテンツ (CPA 対象コンテンツは $M-C+1$〜M) に対し，以下の 4 つの方法のいずれかで要求を発生する．

1. Rand 型: CPA 対象コンテンツの中からランダムに選択したコンテンツを要求
2. Smart fixed 型: 最も低人気のコンテンツから人気の降順にコンテンツを要求
3. Smart rand 型: CPA ホストごとにランダムに始点を決め，人気の降順にコンテンツを要求
4. Smart divide 型: C/N_c の間隔で等間隔に各 CPA ホストの要求開始点を決め，人気の降順にコンテンツを要求

正常ユーザはパラメータ $\theta = 0.7$ の Zipf 分布に従いランダムに選択したコンテンツを要求する．LRU を用いた場合，多様なコンテンツに対し要求が発生するほど多数のコンテンツがキャッシュに挿入される結果，コンテンツの置換が頻発しキャッシュヒット率が低下する．そこで CPA の効果を高めるため，Smart 型の 3 方式はできるだけ特定のコンテンツに集中することなく低人気のコンテンツを要求する．5,500 秒間シミュレーションを行い，100 秒から 5,300 秒の期間に CPA を行う．正常ホストの要求の中でキャッシュから配信できた要求数を正常ホストの要求数で除した値を正常ホストのキャッシュヒット率 Φ と定義し，CPA 対象コンテンツ数 C，CPA ホスト数 N_c，CPA 攻撃強度比 β，Zipf 分布パラメタ θ を変化させたときの Φ を評価する．

図 1 に，C と N_c を変化させたときの Φ をプロットする．ただし *Normal* は CPA を行わない場合の結果である．CPA 対象コンテンツ数 C の増加に伴い，キャッシュに挿入されるコンテンツ数が増加し高人気コンテンツのキャッシュ残存時間が低下する結果，Φ は低下した．しかし C が多くなり M に近づくと高人気コンテンツに対しても CPA の要求が発生するため Φ の低下度合いが弱まった．Smart fixed 型 CPA は，複数の CPA ホストから同一コンテンツに対し同じ時間に要求が発生するため，他の CPA 方式よりも Φ の低下度合いが小さい．

Smart 型方式では，各 CPA ホストは人気の降順にコンテンツを要求するため，各 CPA ホストは短い時間内に同一のコンテンツを要求することはない．そのため N_c が少ないときに Φ の低下が一番大きい．しかし CPA ホスト数 N_c を増加させても Smart fixed 型 CPA 以外の CPA 方式は Φ の変化が小さい．Smart fixed 型 CPA は，CPA ホスト間で要求コンテンツが重複するため，N_c の増加に伴い Φ が大きく増加する．

図 2 に CPA 攻撃強度比 β と正常ホストの要求発生分布の偏り β に対する Φ を各々プロットする．β の増加に伴い Φ は大きく低下した．また θ が増加しコンテンツの人気の偏りが大きくなるにつれて，正常ユーザのヒット率が増加するため Φ は増加するが，CPA の影響は θ の広い範囲で確認される．

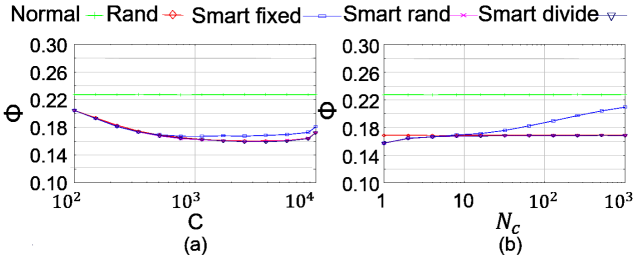

図 1: C と N_c に対する正常ホストヒット率

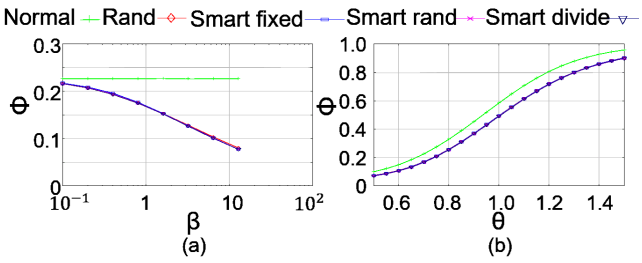

図 2: Φ と θ に対する正常ホストヒット率

4. まとめ

本稿では，CPA のモデルとして 4 つの方式を検討し，正常ホストのキャッシュヒット率低下度合いを計算機シミュレーションにより評価した．その結果，Smart fixed 型以外の 3 つの CPA 方式のキャッシュヒット率低下効果は同等であり，攻撃対象コンテンツ数がコンテンツの総数に対し数 10%程度の広い領域で，また攻撃ホスト数が少ない領域で，その脅威が大きくなることを確認した．今後は，今回得られた CPA の特性を踏まえ，CPA の検知方式に活用したい．

謝辞本研究成果は，JSPS 科研費 18K11283 の助成を受けたものである．ここに記して謝意を表す．

参考文献

[1] S. Paul, A. Seetharam, A. Mukherjee, and M. K. Naskar, Investigating the Impact of Cache Pollution Attacks in Heterogeneous Cellular Networks, IEEE ICNP 2017.

[2] C. Yang, H. Li, L. Wang, and D. Tang, Exploring the Behaviors and Threats of Pollution Attack in Cooperative MEC Caching, IEEE WCNC 2018.