5Gセルラーネットワークにおけるキャッシュポリューション攻撃の検知

Detection of Cache Pollution Attack in 5G Cellular Networks

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

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ことでバックホールのトラヒック負荷を低減することが検討されている [1]. 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.CPA 発生時にはできるだけ迅速に攻撃ホストを特定し, キャッシュを保護することが重要である．そこで限られたメモリ量で高精度に攻撃ホストを特定するため, 本稿ではブルームフィルタを用い CPA を行う端末を検出し防御する方法を提案する．

2. キャッシュポリューション攻撃 (CPA)

CPA とは, 人気のないコンテンツに多数の要求を送ることでネットワーク内のキャッシュの効果を低下させる攻撃である．キャッシュポリューション攻撃には, 大きく分けて二つある．まず一つ目は, すべてのコンテンツに対して一様に要求を行いコンテンツの人気度の偏りを緩やかにすることでキャッシュ性能を下げる False-locality 攻撃である．二つ目は, 攻撃者が低人気のコンテンツから少数の C 個範囲のコンテンツに対し多数要求することでコンテンツの人気の順位を入れ替え, 通常ユーザのコンテンツのヒット率を下げる Loclity-disruption 攻撃である [2,3]. 5G セルラーネットワークの基地局に設置されるキャッシュの容量は限られており, 本来は低人気のコンテンツをキャッシュ対象とさせる False-locality 攻撃の脅威がより大きいと考えられる．そこで本稿では False-locality 攻撃による CPA の検知を目標とする．

3. 提案方式

正常なユーザは短い時間内に同一のコンテンツを複数回，視聴する可能性は低い．一方，CPA の攻撃ホストは短い時間内に同一コンテンツに対し複数回の視聴要求を発生させる．そのため各配信要求に対し，ホスト ID とコンテンツ ID の組をテーブルで管理し，同一ホストからの同一コンテンツに対する配信要求を検知すればよい．しかしユーザ数とコンテンツ数の増加に伴い，管理テーブルに必要となるメモリ量とメモリアクセス回数が急増する．そこでメモリの消費を抑えながら効率的にキーの存在判定が可能であるブルームフィルタを採用する．ホスト ID とコンテンツ ID の組をキーとしてブルームフィルタを用いて，キーの既出現性を判定することで，メモリサイズとメモリアクセス回数を抑えた CPA ホストの検知が可能となる．ブルームフィルタのサイズ B を

$$B = -\frac{n \log p}{(\log 2)^2} \tag{1}$$

ハッシュ関数の個数 k を

$$k = \frac{m}{n} \log 2 \tag{2}$$

により設定する [4]．キャッシュに入る前にコンテンツとホスト ID でブルームフィルタを使い検索を行う. ブルームフィルタによって同ホストが同コンテンツを要求したと判断されなかった場合は, ブルームフィルタにコンテンツとホスト ID を記録し通常通りキャッシュを行う. ブルームフィルタによって同ホストが同コンテンツを要求したと判断された場合は,CPA ホストリストに記録し, キャッシュ対象から外す.

4. 性能評価

M 個のコンテンツに対し, 人気の高いものから順に $1, 2, \cdots, M$ のラベリングがなされている．キャッシュ置換方式は LRU を想定する．コンテンツ数 $M = 10,000$ に対しホスト数 $N = 10,000$ で 1,000 秒間, シミュレーションを行う.N_c 個の CPA 攻撃ホストが存在し，各々はコンテンツの人気順位を把握していることを想定し，300 秒から 600 秒の期間，最も低人気の C 個のコンテンツに対しランダムに CPA を行う．コンテンツとホスト ID を掛け合わせた偽陽性の発生確率 $p = 0.01$ で式 (1)(2) に従いブルームフィルタを設計する. 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．CPA ホストの総要求発生レートは，正常ユーザの総要求発生レートと等しい．攻撃ホストは $M - C \leq m \leq M$ の範囲でランダムに選択したコンテンツを要求する. 攻撃者のユーザ N_c が,10,40 の場合で性能評価をする.

T_{min} を攻撃が開始されてから最初に CPA ホストが検出されるまでに要した時間, T_{av} を攻撃が開始されてから半分の CPA ホストが検出されるまでに要した時間, T_{max} を攻撃が開始されてからすべての CPA ホストが検出されるまでに要した時間と定義する.

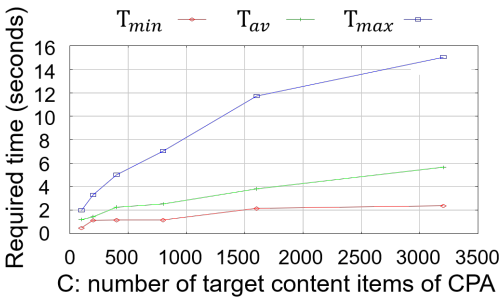

図 1: CPA 検出にかかる時間（$N_c = 10$)

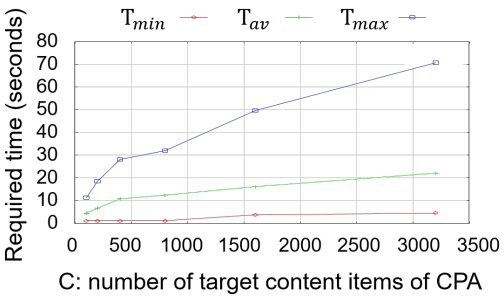

図 2: CPA 検出にかかる時間 ($N_c = 40$)

攻撃対象コンテンツ数や攻撃端末数が少ない場合は, 短時間で検出されるもののそれらが多い時には検出に時間を要する．7.5% の正常ユーザがブルーフィルタの誤検知により誤って規制対象となった．検出に要する時間の短縮と正常ユーザの誤検知の低減のため，今後は，検出閾値を増加した場合やランダムにサンプルした要求に対してのみ検知を行う場合について検討を行う予定である．

[1]G. Paschos, et al., Wireless Caching: Technical Misconceptions and Business Barriers, ComMag, 2016
[2] C. Yang, et al., Exploring the Behaviors and Threats of Pollution Attack in Cooperative MEC Caching, WCNC 2018
[3] S. Paul, et al., Investigating the Impact of Cache Pollution Attacks in Heterogeneous Cellular Networks, ICNP 2017
[4] B. M. Maggs, et al., Algorithmic Nuggets in Content Delivery, ACM SIGCOMM CCR, 45 (3), pp.52 - 66, 2015

Copyright © 2019 IEICE