正常ホストの誤検知低減を考慮した Bloom Filter を用いたキャッシュポリューション攻撃の検知

Detecting Cache Pollution Attack Using Bloom Filter with Reducing False Identification of Normal Hosts

芦原　大和[1]　　上山 憲昭[2]
Takakazu Ashihara　　Noriaki Kamiyama
福岡大学大学院 工学研究科 電子情報工学専攻[1]
Graduate School of Engineering, Fukuoka University
立命館大学 情報理工学部[2]
College of Information Science and Engineering, Ritsumeikan 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、ネットワークの様々な場所にキャッシュサーバを設置しユーザの近くに存在するキャッシュサーバからデータを配信するキャッシュ配信が広く行われている．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キャッシュの効果を低下させる Cache pollution attack (CPA) の問題が指摘されている [1]．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．

そこで筆者らは，少ないメモリアクセス回数で高精度に攻撃ホストを特定するため，ホスト ID とコンテンツ ID の組をキーとする Bloom Filter (BF) を用いた CPA ホストの検知方式を提案した [2]．本方式では，正常ホストの誤検知を抑制するため BF による検知回数に閾値を設けること，また継続的な CPA ホストの検知を可能にするため BF を 2 つ用意して交互に運用することを提案した [2]．しかし正常なホストも同一コンテンツを複数回，視聴する可能性があるが，提案方式では検知回数が時間とともに増加するため，いずれほとんどの正常ホストが誤検知される．そこで本稿では正常ホストの誤検知を防ぐため，検知回数を周期的にデクリメントすることを提案する．提案方式の検知能力を大幅に下げることなく，正常ホストの誤検知を減少させることを示す．

2. 正常ホストの誤検知低減法

[2] で提案した方式は，BF での検知回数に検知閾値 Y を設け，Y 回検知されたホストを CPA として検知する．そのため各ホストの検知回数を記録するためのテーブル (BFDC: BF detection count) を用意する．正常ホストの同一コンテンツの視聴によって BFDC が増加し，やがて CPA ホストとして誤検知することを回避するため本稿では，BFDC の 1 以上のすべてのエントリを，一定周期 P ごとに V だけデクリメントすることを提案する．ただしカウンタ値が 0 となったエントリはそれ以上，減算しない．

3. 性能評価

提案方式の有効性を計算機シミュレーションにより評価する．キャッシュ置換方式は LRU を想定し，コンテンツ数 $M = 20,000$ に対しキャッシュサイズは $1,000$ とする．正常ホスト数 $N = 1,000$ で $6,000$ 秒間シミュレーションを行う．$N_c = 10$ 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，$1,000$ 秒から $5,000$ 秒の期間，攻撃ホストは CPA 対象コンテンツ $C = 1,000$ 個に対して毎秒 5 個の要求を行う．最も低人気の C 個のコンテンツに対し，攻撃対象コンテンツ数/CPA ホスト の間隔で等間隔に各 CPA ホストの要求開始点を決め，人気の昇順にコンテンツを要求する Smart 型で要求を行う [2]．BF の運用開始パラメタ を 0.5 に設定し [2]，BF の偽陽性確率を $p = 0.01$ となるようサイズが 200KB のビットマップを BF 用に 2 個用いる．また BF 検知閾値を $Y = 10$ に，BFDC のデクリメント周期を $P = 100$ 秒に，デクリメント値を $V = 5$ に設定する．正常ホストは，研究室のメンバー 21 人の YouTube の視聴履歴をもとに作成した視聴間隔の分布 [3] に基づき，ランダムに平均視聴間隔を 1,000 個の各正常ホストに設定する．そして各正常ホストに対し，初回要求コンテンツに対する要求確率を管理する．そして要求ごとに，初回要求コンテンツに対する要求か，既要求コンテンツに対する要求かを管理している各集合の選択確率からランダムに選択する．

正常ホストが未要求 (既要求) コンテンツを要求した場合は，未要求 (既要求) コンテンツの中からパラメタ 0.8 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．既要求コンテンツの要求割合の初期値は 0 とし，ホストが既要求コンテンツを要求するごとに，要求コンテンツの要求比率を未要求コンテンツの要求割合で除した値を，その正常ホストの既要求コンテンツの要求割合に加算していく．結果は全て 10 回の試行における平均値で評価する．

BF は偽陽性により，一度も要求をしていないにもかかわらず要求があったと判断される False positive が発生する可能性がある．一方，同じ要求を繰り返したにもかかわらず検知されない False negative は発生しない．正常ホストが提案方式によって誤検知される割合を正常ホストの巻き添え率 σ と定義する．巻き添えの原因は，BF の False Positive に加え，同一ホストが偶然，同一コンテンツを要求した場合にも発生する．

正常ホストのキャッシュヒット率の低下度合い (攻撃強度 η) を評価する．CPA の影響力は，キャッシュヒット率の低下量と，キャッシュヒット率の低下が継続した時間の長さの両方に依存し，各々が大きなほど攻撃強度も高くなる．そこで CPA の攻撃強度を，正常時のキャッシュヒット率と，CPA が行われた場合のキャッシュヒット率との差を，CPA が開始した時刻から，CPA ホストの検知に最も要した時間である $1,000$ 秒後の期間にわたり累積した値で定義する．

表 1 に，検知閾値 Y，デクリメント値 V，デクリメント周期 P のいくつかの組に対し，巻き添え率 σ と攻撃強度 η を各々，まとめる．同じ検知閾値でデクリメント値を増加させると周期的に BFDC がデクリメントするため，正常ホストの巻き添え率が低下する．またデクリメント周期が増加していくと BFDC のカウントアップの期間が増加するため，正常ホストが誤検知され巻き添え率が増加する．

攻撃強度は，検知閾値が同じであれば大きくは変わらない．これは CPA の発生時に攻撃対象コンテンツに対し 2 回目以上の要求が連続して発生するため，デクリメント値の影響しない短い期間で検知されるためである．同じ閾値でデクリメント値が $V = 0$ の場合の攻撃強度が最も高いのは，巻き添え率が高いためである．巻き添え率が高いと正常ホスト数が減少し，CPA ホストの要求数の比率が増加するため攻撃強度が増加する．また P が短いと一つの BF ビットマップを使用中にデクリメントを行うため，一方，P が長いと巻き添え率が増加するため，各々攻撃強度が増加する．

表 1: 正常ホストの巻き添え率と攻撃強度

	σ	η
$Y = 5, V = 0$	0.617	5.445
$Y = 5, V = 2$	0.133	4.643
$Y = 5, V = 5$	0.108	4.512
$Y = 10, V = 0$	0.483	6.286
$Y = 10, V = 5$	0.004	3.451
$Y = 10, V = 10$	0.002	3.453
$Y = 20, V = 10$	0.000	3.486
$P = 10$	0.000	9.214
$P = 50$	0.000	7.945
$P = 200$	0.047	10.195

謝辞 本研究成果は JSPS 科研費 18K11283 と 21H03437 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] A. Takakazu, and K. Noriaki, Detecting Cache Pollution Attacks Using Bloom Filter, IEEE LANMAN 2021.
[3] 芦原大和, 上山憲昭, YouTube の動画の反復視聴行動に関する分析, 電子情報通信学会総合大会, 2021 年 3 月