CDN のキャッシュサーバを騙った DDoS 攻撃の LDNS のログを用いた防御法

DDoS Attacks Deceiving CDN Cache Servers By Checking LDNS Log

谷口 和也[*1]　　上山 憲昭[*2]

Kazuya Taniguchi　　Noriaki Kamiyama

立命館大学 大学院情報理工学研究科[*1]

Graduate Shool of Information Science and Engineering, Ritsumeikan 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

CDN (Content Delivery Network) はインターネットコンテンツを効率的に配信する技術であり，その普及に伴い DDoS (Distributed Denial of Service) 攻撃が増加している [1]．特に攻撃者が CDN の IP アドレスを悪用し，OS (Origin Server) に過負荷をかける攻撃が深刻化している [2]．そこで筆者らは Z スコア法を用いた動的閾値設定による二段階検知手法を提案し，高い検知率と低い処理コストを示した [3]．しかし，ユーザの名前解決要求は LDNS (Local Domain Name System) サーバで実施されるため，権威 DNS サーバのログ確認では正確な判定が難しい．本稿では LDNS サーバでのログ確認の有効性を検討し，キャッシュヒット時のログ欠落リスクを回避する．また，ログ確認処理に伴う遅延時間やサーバ負荷を評価し，複数 OS を標的とした攻撃時の負荷分散効果についても検証する．

2. CDN 使用時の DNS の名前解決処理

CDN を用いている場合，ユーザの配信要求時には CP (Contents Provider) の DNS サーバとの名前解決手順に加え，CDN 事業者の DNS サーバとの間で以下のような手順が生じる．

1. LDNS サーバの要求に対し CP の権威 DNS サーバは CNAME を LDNS サーバへ回答
2. LDNS サーバは CNAME の名前解決を CDN 事業者の権威 DNS サーバへ要求
3. CDN 事業者の権威 DNS サーバは CS を選択しその IP アドレスを LDNS サーバへ回答
4. LDNS サーバはユーザに IP アドレスを回答し，ユーザは指定された CS へアクセス
5. CS にキャッシュされていない場合は，CS は OS からコンテンツを取得してキャッシュ後，ユーザに配信

CS からの正規リクエスト時には経由した DNS サーバに名前解決ログが残るのに対し，ボットネットを用いた不正リクエストでは DNS の名前解決が行われず，ログが残らない．このため DNS ログを解析することで，正規リクエストと攻撃パケットを識別可能である．

3. 提案方式

[3] で提案した方式では，権威 DNS サーバでログ確認を行っていた．しかし，LDNS サーバでキャッシュヒットした場合，権威 DNS サーバを経由しないためログが残らず，適切な検知が難しい．LDNS サーバでログ確認を行えば攻撃の確実な判断が可能だが，都度確認することで遅延が発生する．本稿では，その遅延時間を M/M/1 待ち行列から算出し，処理コストを評価する．遅延時間は伝搬処理とメモリ検索処理に分けて計算する．メモリ検索遅延 T_m は，LDNS サーバのエントリ数 n，1 回のメモリ検索時間 T_r，LDNS 確認回数 c，攻撃継続時間 T_s を用いて，次式で得られる．

$$T_m = \frac{1}{\frac{2}{n \cdot T_r} - \frac{c}{T_s}} \tag{1}$$

また，伝搬遅延 T_d は 1km あたり 5μ 秒の遅延で，権威 DNS サーバと LDNS サーバとの距離を d km とすると，全体の遅延時間 T は次式で得られる．

$$T = 5 \times 10^{-6} d + T_m \tag{2}$$

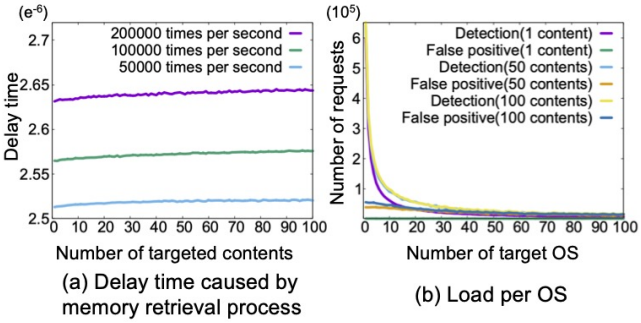

図 1　遅延時間と OS 毎の負荷評価

4. 性能評価

LDNS のログ確認時の遅延と複数 OS を標的とした際の負荷を計算機シミュレーションで評価する．検知には Z スコア法 [4] を用い，短時間に高頻度で発生する攻撃パケットを異常値として検出し，異常値のみ DNS ログ確認を行い処理コストを低減する [3]．正常ユーザは平均 0.005 秒間隔で要求を発生し，シミュレーションは 100 秒間実施する．そのうち 30 秒間は DDoS 攻撃を行い，平均 0.0005 秒間隔で攻撃パケットを複数 OS に分散して送信する．

図 1(a) は，平均 0.0005 秒，0.005 秒，0.001 秒間隔で攻撃パケットを発生させた際のメモリ検索遅延時間を示す．1km あたり 5μ 秒の伝搬遅延と比較して，メモリ検索遅延は数 μ 秒で無視できるほど小さいことが確認された．そのため LDNS サーバにログ確認を行った場合，LDNS サーバまでのネットワークの遅延が，遅延時間として発生する．

図 1(b) は，複数 OS を標的に攻撃範囲を 1〜100 で変化させた際の各 OS の負荷を示す．総攻撃パケット数は一定で，標的コンテンツ数 1，50，100 の場合の検知数と誤検知数を評価した．標的 OS 数が増加すると攻撃が分散され，各 OS の負荷は低減する．攻撃効率は単一 OS を標的とする方が高い．また，標的コンテンツ数 100 では検知負荷が最も高く，攻撃効果の向上が示唆された．今後は攻撃者にとって最適な攻撃コンテンツ数について評価する予定である．

謝辞　本研究成果は JSPS 科研費 23K11086，23K21664，23K28078 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] D. Wagner，et al., United We Stand: Collaborative Detection and Mitigation of Amplification DDoS Attacks at Scale，CCS 2021

[2] M. Ghaznavi，et al., Content Delivery Network Security: A Survey，IEEE Communications Surveys & Tutorials, Vol. 23, No. 4, 2021

[3] 谷口 和也，上山 憲昭，CDN のキャッシュサーバを騙った DDoS 攻撃の二段階検知法，信学会 NS 研究会，NS2023-222，2024 年 2 月

[4] C. Hou，et al，A Wind Direction Forecasting Method Based on Z Score Normalization and Long Short Term Memory，ICGEA 2019