CDN のキャッシュサーバを騙った DDoS 攻撃の Z スコア法を用いた二段階検知による防御法

DDoS attacks that deceive CDN cache servers are prevented by a two-step detection method using the Z-score method.

谷口 和也　　上山 憲昭
Kazuya Taniguchi　　Noriaki Kamiyama
立命館大学　情報理工学部　情報理工学科
Faulty 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キャッシュし，効率的に配信する技術である．近年 CDN の普及に伴い，DDoS(Distributed Denial of Service) 攻撃が増加しており，攻撃者が CDN ネットワークを標的とするケースも報告されている [1]．攻撃者が CDN の IP アドレスを悪用し，直接 OS(Origin Server) に過負荷をかける攻撃が深刻な脅威となっている [2]．[3] で著者らは，リクエストの発生パターンの差異に着目し，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，高い検知率と処理コストの低減を示した．本稿では，新たに LDNS(Local Domain Name System) サーバにおけるログ確認の有効性を検討する．権威 DNS ではなく LDNS でのログ確認を行うことで，キャッシュヒット時のログ欠落リスクを回避する．ログ確認処理に伴う遅延時間およびシステム負荷について評価を行う．さらに先行研究では，単一の OS を標的とした攻撃を発生させていたため，本稿では複数の OS に対し同量の攻撃トラフィックを仕掛けた場合についてシミュレーションし，提案方式に対しては単一 OS を攻撃した方が有効であることを示した．

2. 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 サーバとの間で手順が生じる．CDN の名前解決の手順について示す．

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] で著者らが提案した方式では，権威 DNS サーバでのログの確認処理を行なっていたが，名前解決の処理時に LDNS サーバでキャッシュヒットすると，権威 DNS サーバを経由しないことによってログが残っておらず，適切な検知処理が行えない．LDNS サーバでログ確認することで確実に攻撃かを判断することが可能である．しかし毎回確認しにいく必要性があるため，遅延が発生することが推測される．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．また遅延時間の計算では伝搬処理とメモリ内の検索処理に分け算出する．伝搬遅延である 1km あたりの伝搬で 5 μ s の遅延とし，メモリ内の検索処理で生じる遅延時間 T は，LDNS サーバのエントリ数を n、一つのメモリ検索時間を T_r，シミュレーション中に LDNS に確認する回数を $count$, 継続時間を T_s とすると，

$$T = \frac{1}{\frac{2}{n \cdot T_r} - \frac{\mathrm{count}}{T_s}} \tag{1}$$

で示される．

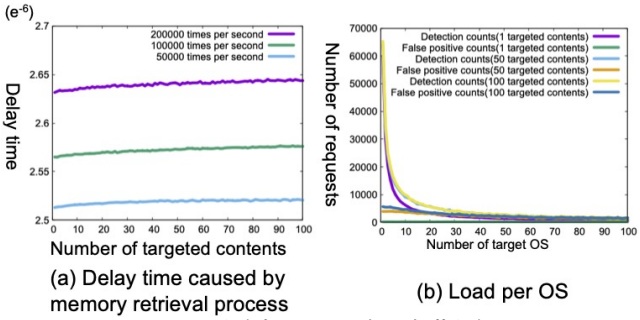

図 1　遅延時間と OS 毎の負荷評価

4. 性能評価

本稿は，[3] で提案された Z スコア法を用いた動的閾値設定による DDoS パケット棄却法の検知性能と負荷評価を目的とする．LDNS の名前解決ログ確認時の遅延評価に加え，複数 OS を標的とした場合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 ログ確認を行うことで処理コストを低減する [4]．正常ユーザは平均 0.005 秒の指数分布に従い要求を発生させる．シミュレーションは 100 秒間行い，そのうち 30 秒間は DDoS 攻撃を設定し，平均 0.0005 秒の指数分布に従い攻撃パケットを分散して標的に送信する．

(a) はメモリ検索処理における遅延時間を示している．1km あたり 5 μ s の遅延を考慮した伝搬遅延と比較すると，提案方式におけるメモリ検索処理の遅延時間は占有率が低いことが確認された．また，権威 DNS サーバから LDNS サーバにログ確認の対象を変更しても，システム運用上において大きな性能劣化は生じず，実用上の支障はほとんどないことが示された．(b) は複数の OS を標的とする攻撃シナリオを想定し，攻撃範囲を 1 から 100 の範囲で変化させた場合の各 OS における負荷を示している．標的 OS の数を増加させることで攻撃数が分散され，各 OS への負荷が低減することが確認された．攻撃者の視点からは，単一 OS に標的を絞る方が攻撃効率は高いと考えられる．一方で，標的コンテンツ数を増加させることで攻撃の効果が向上する可能性も示唆されるため，ネットワーク環境に応じた標的コンテンツ数の最適値が存在すると考えられる．

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, D. Kopp, M. Wichtlhuber, C. Dietzel, O. Hohlfeld, G. Smaragdakis, A. Feldmann, United We Stand: Collaborative Detection and Mitigation of Amplification DDoS Attacks at Scale, CCS '21: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security
[2] M. Ghaznavi, E. Jalalpour, A. Salahuddin, R. Boutaba, D. Migault, S. Preda, Content Delivery Network Security: A Survey, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 23, NO. 4, FOURTH QUARTER 2021
[3] 谷口和也，上山憲昭，CDN のキャッシュサーバを騙った Z スコアを用いた検知法，信学会 2023 年総合大会，B-7-28
[4] C. Hou, H. Han, Z. Liu, and M. Su, A Wind Direction Forecasting Method Based on Z Score Normalization and Long Short Term Memory, ICGEA 2019.