CDN のキャッシュサーバを騙った DDoS 攻撃の Z スコアを用いた検知法

Detecting DDoS Attack Mimicking CDN Caches Using Z Score

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

今日のインターネットトラフィック総量に占めるビデオトラフィックの割合は増加し続けており 80% を超えている．ユーザ数とコンテンツのサイズの増加に伴い，コンテンツプロバイダやネットワーク事業者は，安定した品質を提供し続けるための設備投資の増加，運用コストの増加が問題となっている．さらに，要求ユーザとコンテンツを提供するオリジンサーバ（OS）との間に大きな地理的距離がある場合，大きな遅延が発生し QoS（Quality of Service）が低下する可能性がある．これらの問題に対処するため，多くのコンテンツプロバイダはサービス CDN（Content Delivery Network）を用いている．

一方で近年，ネットワーク上に広く存在するボットから大量のパケットをターゲットホストに送信することで，ターゲットサーバを機能不全とする DDoS（Distributed Denial of Service）攻撃が頻繁に発生している．CDN ではユーザの配信要求に対し，選択されたキャッシュサーバ（CS）に要求コンテンツが存在しない場合のみ OS に要求が届く．そのためボットが標的 OS に直接パケットを送信した場合，CS 以外からの配信要求をファイアウォールで棄却することで DDoS に対処できる [1][2]．しかしボットが CS の IP アドレスを発アドレスとして偽り OS へパケットを送信した場合は，ファイアウォールで検知できない．

CS からの正常な問い合わせ時には，コンテンツ提供者の DNS サーバに名前解決のログが残るが，ボットからの直接要求は DNS の名前解決を用いないため名前解決のログが残らない．そのため DNS のログを調べれば，CS からの正常な配信要求か，ボットからの DDoS パケットか判別可能である．しかし全ての配信要求に対して DNS のログを調査すると，その処理コストの増大が問題となる．そこで著者らは DDoS 攻撃のパケットが短い時間間隔で多数発生することに着目し，到着時間間隔に対して閾値を設け，閾値以下の間隔で同一 IP アドレスから要求が到着した場合にのみ DNS のログをチェックする，CDN を騙った DDoS 攻撃の二段階検知法 [3] と最適閾値設計法を提案した [4]．しかし一般的に配信要求の発生パタンは動的に変化するが，本方式では閾値を固定的に設定するため，動的な環境に対する対処が困難である．そこで本稿では動的な環境への対応が可能な Z スコア [5] を用いた二段階検知法を提案する．

2. Z スコア法

Z スコアはデータの外れ値を検知するアルゴリズムである [5]．過去の直近のデータから移動平均と標準偏差を更新し，大きく平均から外れた値を検知し，アラームを発生する．Z スコア法のアルゴリズムを下記に記す．

$$S_i = \begin{cases} 1, & E_c - \mu_{i-1} > \eta\delta_{i-1} \\ -1, & E_c - \mu_{i-1} < \eta\delta_{i-1} \\ 0, & otherwise \end{cases} \quad (1)$$

$$E_i = \begin{cases} E_c, S_i = 0 \\ \alpha \times E_c + (1-\alpha) \times E_{i-1}, otherwise \end{cases} \quad (2)$$

$$\mu_i = mean(E_{i-L+1}, E_{i-L+2}, \cdots, E_i) \quad (3)$$

$$\delta_i = std(E_{i-L+1}, E_{i-L+2}, \cdots, E_i) \quad (4)$$

ラグ L は考慮する過去のデータの個数である，閾値 η は信号を検知する際の感度である．影響 α は検出時の信号補正における信号の影響の強さである．過去 L 期間の想定値から計算された平均と標準偏差を用いて外れ値を検知し，外れ値として検知された測定値を直前の測定値との重みづけ和に更新する．

3. Z スコアによる DDoS 攻撃検知法

提案方式は Z スコア法を用いて DDoS 攻撃を検知する．コンテンツの要求が OS に到着した際に，そのコンテンツに対しての直前の要求との到着間隔を記録する．Z スコア法は測定値と平均値との差異が大きな場合に検知するが，通常のコンテンツ要求と比較して，DDoS 攻撃では短い時間間隔で要求が到着する傾向があり，到着間隔を Z スコアの測定値に用いると DDoS が検知できない．そこで到着間隔の逆数を Z スコア法の入力 E_c に用いる．

そして到着した要求が外れ値かどうかを Z スコアを用いて検査し，アラームが発生した場合は, 攻撃の可能性があると判断して DNS のログを確認し, 最終的な攻撃判断を行う．攻撃の継続中は，要求の到着間隔が正常な要求だけの時とは異なり，攻撃データを用いて過去 L の平均や標準偏差を更新すると, Z スコアの検知に用いる平均や標準偏差が歪む．そこで攻撃検知後は，Z スコア法での平均値や標準偏差の更新を行わない．そして DNS ログ検査の結果，連続して P 回，正常な要求と判断された場合に，攻撃が終了したと判断し，平均値と標準偏差の更新を再開する．このような方法を用いることで, 攻撃が発生する前の正常な要求だけのデータを用いた外れ値の検査が可能となる．

4. 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て評価する．キャッシュ置換方式は LRU 方式とし，コンテンツ数を $N = 100$, シュミレーション時間を 10,000 秒とする．また正常ユーザからは平均 1 秒の指数分布に従う間隔で要求を発生させた．Z スコアのパラメタは，$L = 5$, $\eta = 1.0$, $\alpha = 0.5$ に設定した．3,000 秒から 6,000 秒の間に DDoS 攻撃を発生させ，その期間中は平均が 2 秒または 3 秒の指数分布に従う間隔で DDoS の要求パケットを特定のコンテンツに対して発生させた．また，攻撃検知後の攻撃終了判断に用いる P は $P = 5$ に設定した．

表 1 に，DDoS パケットの各々の平均到着間隔において，DDoS パケットを検知できた割合 (検知確率) と，正常パケットを誤って DDoS の可能性ありと検知した割合 (誤検知率) を示す．提案方式を用いることで，正常パケットの誤検知率を 10% 程度に抑えながら，ほぼ全ての DDoS パケットが検知可能なことが確認できる．なお，正常パケットが誤検知された場合であっても，DNS ログの確認により最終的に誤検知されるパケットをゼロにできる．

表 1　DDoS パケットの検知率と正常パケットの誤検知率

DDoS の平均到着間隔	2 秒	3 秒
DDoS パケットの検知率	99.9%	99.9%
正常パケットの誤検知率	8.2%	12.7%

謝辞本研究成果は JSPS 科研費 18K11283 および 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] T. Vissers, et al., Maneuvering Around Clouds: Bypassing Cloud-based Security Providers, ACM CCS 2015
[2] D. Gillman, et al., Protecting Websites from Attack with Secure Delivery Networks, Comp. Mag., 2015
[3] 宮崎椋平，上山憲昭，CDN のキャッシュサーバを騙った DDoS 攻撃の防御方式，信学会 2021 年総合大会，B-11-10
[4] 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の最適閾値設定法，信学会 2022 年ソサイエティ大会，B-14-7
[5] 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.