CDN を利用した DDoS 攻撃の Z スコアを用いた検知法の性能評価

Performance Evaluation of Z-Score Based Detection Method of DDoS Attack Using CDN

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

近年，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．一方でコンテンツ配信の高速化・経済化の目的から CDN (Content Delivery Network) がコンテンツ配信に広く用いられているが，CDN を配信に用いるコンテンツのオリジンサーバ (OS) に対する DDoS 攻撃は，攻撃パケットが多数のキャッシュサーバ (CS) に分散するため，CDN は DDoS 攻撃の防御にも有効である．しかしボットが標的 OS に直接パケットを送信した場合 DDoS 攻撃が成立する．通常は CS 以外からの配信要求を OS に設置した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．

そこで著者らは，Z スコアを用いた DDoS 攻撃の二段階検知法を提案した [3] が，性能評価が限定的である．そこで本稿では [3] で提案した検知法による DDoS 攻撃の検知精度を評価し，提案方式の有効性を確認する．

2. 提案方式

提案方式では，閾値の設定法にデータの外れ値を検知するアルゴリズムである Z スコア法 [4] を用いる．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 スコア法を用いることで過去のデータを反映した外れ値検知を実現でき，正常なコンテンツ配信要求と DDoS 攻撃の要求発生パターンの違いを検知することが可能になる．

提案方式は DNS の名前解決ログでの検知に加え，OS の負荷軽減を目的とした Z スコア法を用いた動的な閾値設定により DDoS パケットを検知する．まず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 スコアで判定し，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知が可能となる．

本稿では，処理負荷をオーダ表記により比較することで提案方式の処理負荷軽減の妥当性を確認する．提案方式を用いた場合，Z スコアの計算処理により DDoS パケットを検知することができる．Z スコアは単純な計算式であるため，平均値と標準偏差を事前に計算することで瞬時に結果を出力可能で，Z スコアアルゴリズムの時間計算量は入力数に依存しない．したがって，Z スコアアルゴリズムの時間計算量は $\mathcal{O}(1)$ となる．また，DNS ログの検索方式は様々であるが，線形探索を想定するとエントリ数 n に対して DNS ログの検索処理の最悪時間計算量は $\mathcal{O}(n)$ となる．これらを比較すると，提案方式においては Z スコアによる検出処理が DNS ログの検査処理と比較して処理負荷が小さく，提案方式を用いることで計算量の低減が可能である．

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 $N = 100$，キャッシュ容量を $C = 10$ 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る．Z スコアのパラメタは，$L = 10$，$\eta = 4.0$，$\alpha = 0.5$ に設定した．計算機シミュレーションを 10,000 秒実行し，期間中の 3,000 秒間 DDoS 攻撃を発生させ，その期間中は設定した平均発生間隔 D 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閾値は $P = 5$ に設定した．Z スコアの学習時間に対する検知率の低減を調査した結果，5,000 秒の学習時間で検知率の低下は見られず，適切に学習できていた．そのため攻撃を開始するまでに 5,000 秒の学習時間を設けた．

性能評価では，人気度の異なるコンテンツが攻撃対象になった場合のコンテンツ毎の検知能力を評価する．DDoS パケットの平均発生間隔を，0.5，1.0，5.0，10.0 秒の 4 パターンに設定し，指数分布に従う間隔で DDoS パケットを特定のコンテンツに対して発生させた．

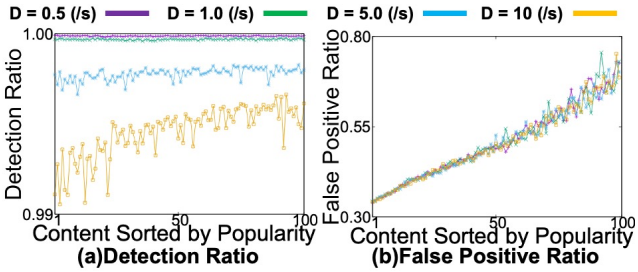

図 1　各ターゲットコンテンツにおける検知率と誤検知率

図 1 に各コンテンツに対して DDoS 攻撃が発生したときの，(a)DDoS パケットを Z スコア法で検知できた確率 (検知率) と，(b) 正常パケットを Z スコア法で誤って検知した確率 (誤検知率) を，各ターゲットコンテンツの人気度の降順にプロットする．提案方式は到着間隔に着目しているため，高人気コンテンツの方が検知困難と推測できるが，図 1(a) より，攻撃対象の人気度に関わらず 0.99 以上の高い検知率を維持している．一方図 1(b) より誤検知率が 0.3 0.8 と高いが，提案方式では Z スコアで検知された後に DNS の名前解決のログにより攻撃かの判定が誤検知なしで可能であり，正常なコンテンツ配信要求を誤って棄却することはない．高人気コンテンツに対する攻撃では誤検知率が 0.3 程度となっていることから，最も正常ユーザの要求数が多い高人気コンテンツのパケットの 7 割程度を DNS のログを確認することなく，正常パケットと判断可能である．

謝辞本研究成果は JSPS 科研費 21H03436 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]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] 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, et al., A Wind Direction Forecasting Method Based on ZScore Normalization and Long Short Term Memory, ICGEA 2019