令和4年度　春学期　卒業研究3 (BI)
学士論文

題目 CDNにおけるDDoSの攻撃パケット検知法

指導教員 上山憲昭 教授

立命館大学 情報理工学部 セキュリティ・ネットワークコース

学籍番号 TL181272
谷口和也

令和5年1月31日

概要

インターネット上ではコンテンツの多くが，遅延時間とトラヒック量を削減するため，CDN（Content Delivery Network）を用いて配信されている．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．そのような攻撃に対して，ボットが OS の IP アドレス宛てに直接パケットを送信した場合は，OS に対し CS から要求が届くことから，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対処できる．しかし，ボットがキャッシュサーバ（CS）の IP アドレスを発アドレスとして偽り，標的オリジンサーバ（OS）へパケットを送信した場合に，ファイヤーウォールで検知ができない問題がある．それに対して著者らは，DDoS 攻撃が短い時間間隔で多数の CS から発生することに着目し，要求発生の違いを利用した，CDN を騙った DDoS 攻撃の二段階検知法を提案した [1]. そこで，本稿では，先行研究では扱われていなかった一段階目の判別として利用する閾値の設定法を提案する．また, その他の DDoS 攻撃の防御法として Z スコアアルゴリズムを活用し，到着間隔をデータとして外れ値を検知することによって，DDoS 攻撃が短い時間間隔で発生する特性により攻撃が発生した時を検知するという Z スコアを活用した DDoS 攻撃の防御法について提案する．

目 次

第1章　序論

1.1　研究の背景

今日のインターネットトラフィックの総量に占めるビデオトラフィックの割合は増加しており，2019 年には約 80 %に達すると予測されている．この傾向は，ネットワークオペレーター，特にコンテンツプロバイダーに影響を与えている．ユーザー数とコンテンツのボリュームが増加するにつれて，コンテンツプロバイダーは，集中型のクライアントサーバーアーキテクチャを使用してマルチメディアサービスを提供し，コンテンツの処理と送信の負荷に問題となっている．さらに，クライアントとサーバーの間に大きな地理的距離がある場合，クライアントで大きな遅延が発生し，QoS（Quality of Service）が低下する可能性がある．上記の問題を克服するために，コンテンツプロバイダーはサービスに CDN テクノロジを採用している [2]．また近年，DDoS（Distributed Denial of Service）攻撃が頻繁に発生している．DDoS 攻撃は，多数のマシンによって大量のトラフィックを生成することによって被害者をフラッドさせようとする試みである．DDoS 攻撃には，保護されていないコンピューターに悪意のあるソフトウェアを植え付けることによって，高速接続を介してインターネットにアクセスする保護されていないコンピューターから収集されたゾンビまたはボットと呼ばれる侵害された多数のホストが使用される．これらのホスト（ゾンビまたはボット）をグループ化して，ボットネットと呼ばれる 1 つの巨大なネットワークを形成する．ボットネットは，さまざまな動機（恐喝, 復讐, または悪意）を持つ攻撃者からのコマンドのみを待って，DDoS 攻撃を開始する [3]．そのような攻撃に対して，通常，ボットが OS の IP アドレス宛てに直接パケットを送信した場合は，OS に対し CS から要求が届くことから，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対処できる．しかし，ボットがキャッシュサーバ（CS）の IP アドレスを発アドレスとして偽り，標的オリジンサーバ（OS）へパケットを送信した場合に，ファイヤーウォールで検知ができない問題がある．本稿では，上記のような問題を解決する方式を提案する．

1.2　研究の目的

DDoS 攻撃では，通常ボットが OS の IP アドレス宛てに直接パケットを送信した場合は，OS に対し CS から要求が届くことから，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対処できる．しかし，ボットがキャッシュサーバ （CS）の IP アドレスを発アドレスとして偽り，標的オリジンサーバ（OS）へパケットを送信した場合に，ファイヤーウォールで検知ができない問題がある．このような DDoS 攻撃が短い時間間隔で多数の CS から発生することに着目し，要求発生の違いを利用することで DDoS 攻撃を検知すること目的とし、本稿では先行研究である DDoS 攻撃の二段階検知法での一段階目の判別として利用する閾値の設定法を提案する．また, その他の DDoS 攻撃の防御法として Z スコアアルゴリズムを活用し, 到着間隔をデータとして外れ値を検知することによって, DDoS 攻撃が短い時間間隔で発生する特性により攻撃が発生した時を検知するという Z スコアを活用した DDoS 攻撃の防御法について提案する．

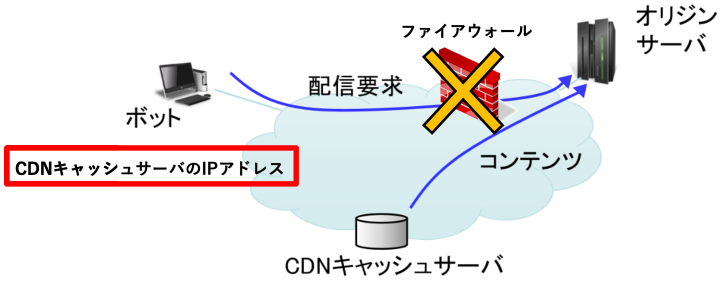

図 1.1: IP アドレスを発アドレスとして偽った攻撃の様子

第2章　関連研究

2.1　CDN の名前解決法

CDN を用いている場合，ユーザの配信要求時には CP 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 (Local DNS) 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

そのため CS からの正常な問い合わせ時には，CP の DNS サーバに名前解決のログが残るが ，ボットからの OS の IP アドレスを直接用いた要求は DNS の名前解決を用いないため名前解決の履歴が残らない．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 パケットかの区別が可能である．しかし，OS には大量の配信要求が到着することから，すべての配信要求に対して DNS のログを調べると OS の処理負荷の増大が懸念される.

2.2　DDoS 攻撃の二段階検知法

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のに対し，ボットからの IP アドレスを直接用いた要求は 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 パケットか判別が可能である．しかし, OS には大量の配信要求が到着することからすべての配信要求に対して DNS のログを調べると OS の処理負荷の増大が懸念される．そのため，先行研究では問い合わせ間隔に閾値 T を設定し，ホストごとに要求の到着間隔の計測を行い，T に対しての要求の到着間隔の長さにより DNS サーバの問い合わせの有無を確認する必要のある要求を絞り込んでいる．具体的な判別の方法としては，T より長い間隔の要求は CS からの正常な要求と見做し, T より短い間隔の要求はボットからの DDoS 攻撃の可能性を考え問い合わせの有無を確認する．さらに問い合わせが有れば CS からの正常な要求と見做し，問い合わせがなければ DDoS 攻撃と見做しアクセスを棄却する．本方式により DNS のログの検索負荷を減らし，DDoS 攻撃を効率よく検知することができる [1].

2.3 Z スコアアルゴリズム

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 [4]．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.

$$S_i = \begin{cases} 1, & E_c - \mu_{i-1} > \eta\delta_{i-1} \\ -1, & E_c - \mu_{i-1} < \eta\delta_{i-1} \\ 0, & otherwise \end{cases} \tag{2.1}$$

$$E_i = \begin{cases} E_c, S_i = 0 \\ \alpha\times\ E_c + (1-\alpha) \times E_{i-1}, otherwise \end{cases} \tag{2.2}$$

$$\mu_i = mean(E_{i-L+1}, E_{i-L+2}, ..., E_i) \tag{2.3}$$

$$\delta_i = std(E_{i-L+1}, E_{i-L+2}, ..., E_i) \tag{2.4}$$

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．

表 2.1: Z スコアアルゴリズムの式の記号と定義

記号	定義
S_i	信号
E_c	実際のデータ
E_i	Z スコア導入後のデータ
μ	過去のデータからの平均
η	閾値
δ	過去のデータからの標準偏差
α	影響
L	ラグ

第3章　提案方式

3.1　二段階検知法の最適閾値設定法

3.1.1　概要と特徴

先行研究である DDoS 攻撃の二段階検知法では，閾値 T を大きく設定しすぎると DNS サーバでの問い合わせの有無を確認する回数が増え OS の負荷が増大する．一方，閾値 T を小さく設定しすぎると DDoS 攻撃を検知できない可能性があり，DDoS 攻撃に対しての強度が低下するという問題がある．その問題に対し，本稿では閾値 T を最適なものに設定するということに着目している．上記を満たすためには，閾値 T は DNS の検査レートの許容上限を満たす範囲で最大化することが必要になってくる．このように閾値を設定することで，DNS サーバの処理能力上限を考慮しながら，DDoS 攻撃を最大限，検知することができる．DNS サーバの処理能力上限とは，コンテンツ毎の DNS 検査レートを全てのコンテンツに対して考慮したものになる．ここでは DNS の総検査レートとする．最適な閾値 T を求めるには，DNS の総検査レートが必要になる．検査コンテンツ数を M，閾値 T に対してのコンテンツ m の DNS の検査レートを $r_m(T)$ とすると，T に対する DNS の総検査レート R_n は

$$R_n(T) = \sum_{m=1}^{M} r_m(T) \tag{3.1}$$

で求まる．この DNS の総検査レートを用いて，DNS の検査レートの上限値を U_n とするとき，$R_n(T) = U_n$ となる T の最大値を T に設定する．こうすることで最適な閾値 T が求まる．

3.2　Z スコアによる DDoS 攻撃検知法

3.2.1　概要と特徴

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．

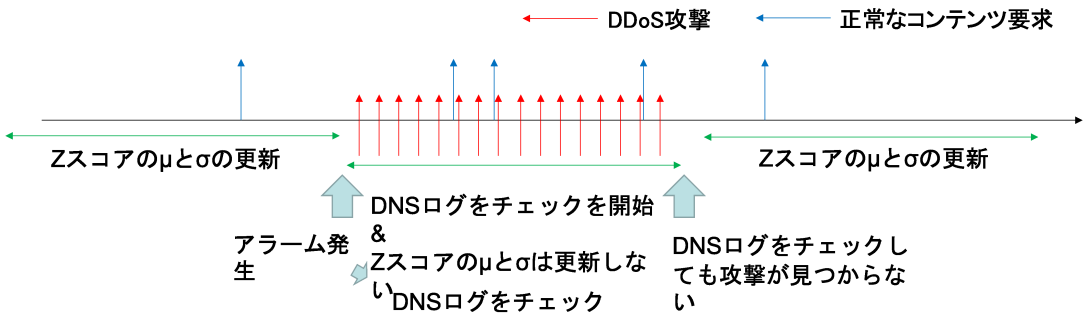

図 3.1: Z スコアによる DDoS 攻撃検知法

第4章　性能評価法

4.1　二段階検知法の最適閾値設定法

二段階検知法の最適閾値決定法の有効性を計算機シュミ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，ユーザのコンテンツ選択確率はパラメタθのZipf分布に従う．シミュレーションでは，さまざまなパラメタでの結果を出力するため，$CS = 5, 10, 15$と$\theta = 0.5, 0.8, 1.2$の合計9パターンでシミュレーションを行っている．

二つの観点から評価を実施する．

CSやZipf分布のθを変化させたときのコンテンツ毎のキャッシュミスの発生間隔の平均値において評価を行う．この観点により，パラメタを変化させたときのコンテンツ毎のキャッシュミスの状態を確認できる．これにより，Zipf分布のθが大きく，高人気コンテンツの要求比率が高い場合は，高人気コンテンツのキャッシュミスが減少するという推測との比較により計算機シュミレーターの有効性を評価できる．

CSやZipf分布のθを変化させたときの上限値を満たす最適な閾値Tにおいて評価を行う．閾値Tはコンテンツの到着間隔より危険性を判別し，DNSのログの確認する要求OSの負荷を軽減するものなので提案方式の有効性を評価できる．上限値を満たす最適な閾値Tをグラフにプロットすることで，閾値を仮に設定した際のコンテンツ全てに対してのDNSの総検査レートのグラフより閾値を設定した際のグラフとの交点から求めることができる．

4.1.1　Zスコアによる DDoS 攻撃検知法

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100秒とする．また正常ユーザからは平均1/100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，通常$L = 5$，$\eta = 1.0$, $\alpha = 0.5$に設定した．30秒から60秒の間にDDoS攻撃を発生させ，その期間中は平均が1/100，1/50，1/20，1/10，1/5秒の5パターンの指数分

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．

性能評価では，コンテンツを変化させたときと閾値 $\eta = 0.5$ に変更した場合の 2 パターンにおいてシミュレーションを行っている．コンテンツを変化させたときの条件では，RANK5 と RANK15 のコンテンツをデータとして扱っている．RANK とはコンテンツの人気度を示していて，RANK5 とは 5 番目に人気度の高いコンテンツを指している．着目するコンテンツを変更すると正常パケットの平均到着間隔が変わるため到着パターンの違いをどの程度検知できるかを評価できる．また，閾値を変更するのは，Z スコア法の感度との関連性を評価するため行っている．閾値を小さく設定することで外れ値を検知しやすくなっているので，DDoS パケットを多く検知できる．しかし，その反面正常パケットの誤検知も増えてしまうことが予測される．評価点として，各条件下における DDoS パケットの検知率と正常パケットの誤検知率において評価を行う．DDoS パケットの検知率とは到着した DDoS パケットに対しての Z スコア法で危険であると検知できた割合を表している．正常パケットの誤検知率とは，要求の到着間隔から正常パケットを危険性があると誤ってみなした割合である．しかし，正常パケットの誤検知に関しては，危険性があるとみなした後に，DNS のログの確認を行うことで DDoS パケットかどうかの判別を確実に行えるので，誤って棄却してしまう危険性はない．

第5章　結果

5.1　二段階検知法の最適閾値設定法

5.1.1　キャッシュミスの平均発生間隔

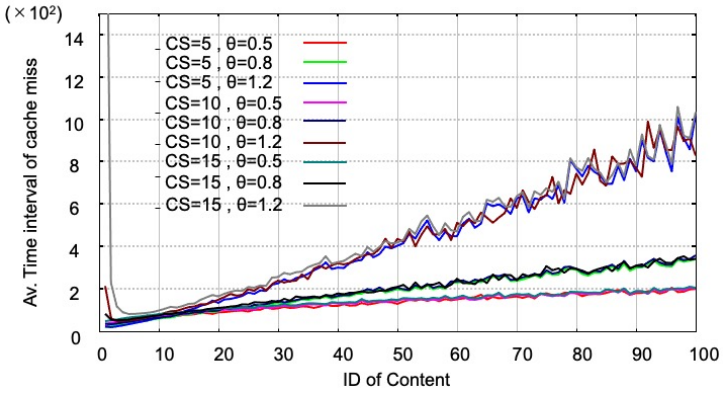

図 5.1: キャッシュミスの平均発生間隔

上図は CS や Zipf 分布の θ を変化させたときのコンテンツ毎のキャッシュミスの発生間隔の平均値を示している．コンテンツ ID は人気順を示していて，低くなるほど人気度が高くなる．従って，コンテンツ ID が大きくなるほどキャッシュミスの発生回数が少なくなるためキャッシュミスの発生回数の平均値が大きくなるのは予想できる．上図から推測と同様にコンテンツ ID が大きくなるほどキャッシュミスの発生回数の平均値が大きくなっていることがわかる．しかし一方で，特に Zipf 分布の θ が大きく，高人気コンテンツの要求比率が高い場合は，高人気コンテンツのキャッシュミスが減少するため，キャッシュミスの発生間隔が増加する．そのため CS や Zipf 分布の θ を大きく設定してものでは，平均キャッシュミス発生間隔は下に凸な曲線となっていることがわかる．

5.1.2　上限値に対する最適な閾値 T

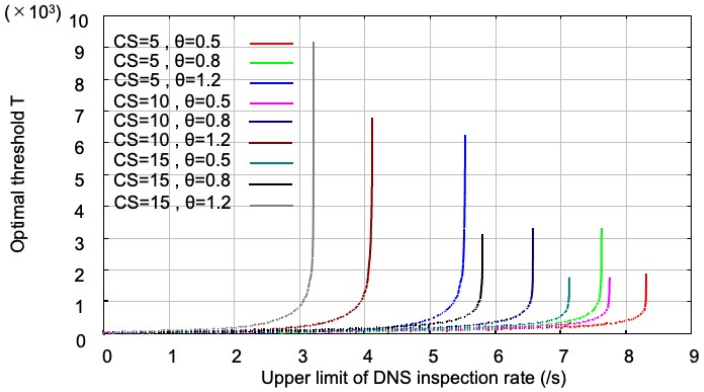

図 5.2: 上限値に対する最適な閾値 T

上図は CS や Zipf 分布の θ を変化させたときの上限値を満たす最適な閾値 T を示したものである．これは，閾値を仮に設定した際の特定のコンテンツにおける DNS の総検査レートから求めたものである．シミュレータでは，シミュレーション時間を設定しているため途中で途切れているが，シミュレーションを継続すると直前までのように指数関数的に増加する．CS や Zipf 分布の θ を変化させても大きな変化はなく，いずれの場合も上限値の増加に伴い T の最適値は増加するが，上限値がある値に近づくと急激に T の最適値は増加する．

5.2　Z スコアによる DDoS 攻撃検知法

5.2.1　コンテンツを変更したときの結果

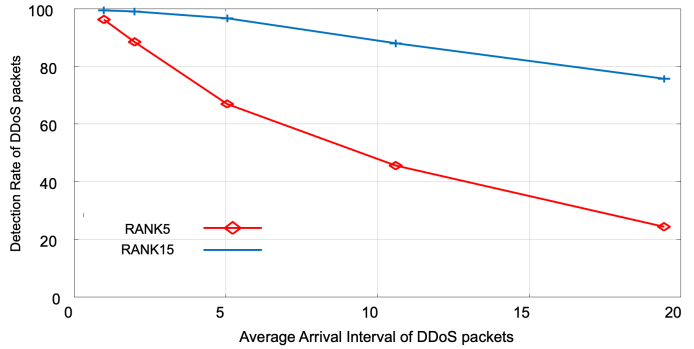

図 5.3: コンテンツを変更したときの DDoS パケットの検知率

上図は RANK5 と RANK15 のコンテンツでの DDoS パケットの検知率を示している．コンテンツを変更したときの DDoS パケットの検知率の結果より，RANK5 の様に正常パケットの到着間隔が短いものだと短い時間で連続して発生する DDoS 攻撃との判別が困難で，見逃しも多くなってしまっている．しかし，RANK15 に関しては，RANK5 よりも比較的良い結果になっており，攻撃の間隔が短い時は全て検知できている．

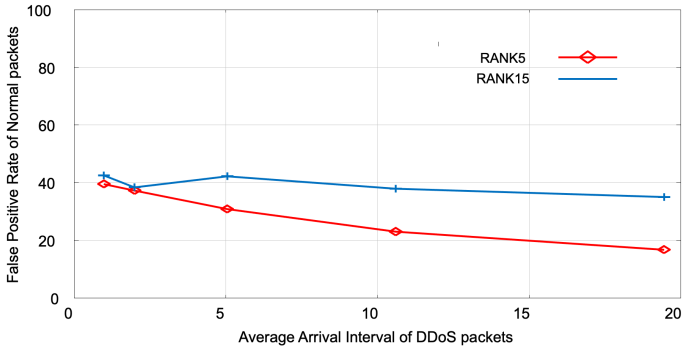

図 5.4: コンテンツを変更したときの正常パケットの誤検知率

上図は，RANK5 と RANK15 のコンテンツでの正常パケットの誤検知率を示している．コンテンツを変更したときの正常パケットの誤検知率より，到着間隔が大きい方が正常パケットの誤検知率が低いことがわかる．これは，平均到着間隔が大きくなるため検知しやすくなってしまうためである．また，人気度の高いコンテンツの方が全体的に正常パケットの誤検知率が低いのは，正常パケットを学習する際に大きい到着間隔で学習しているため，攻撃発生中に検知しやすくなっているためである．

5.2.2 Z スコア法の閾値を変更したときの結果

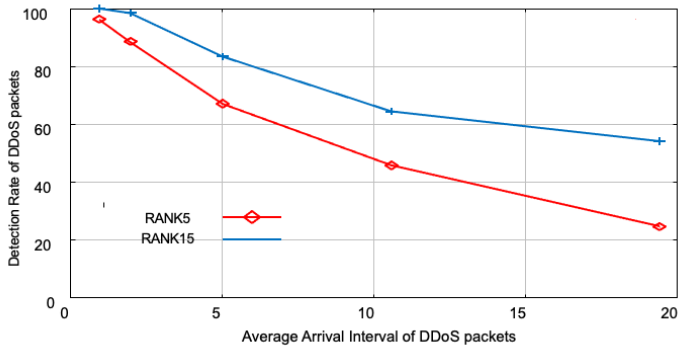

図 5.5: Z スコア法の閾値を変更したときの DDoS パケットの検知率

上図は RANK5 のコンテンツに対して，$\eta = 1.0$ と $\eta = 0.5$ で Z スコア法を適応し検知をおこなった際の DDoS パケットの検知率を示している．性能評価で予想していたのと同様に，閾値を小さく設定することで外れ値を検知しやすくなっているのため，DDoS パケットを多く検知できている．しかし，到着間隔が大きくなると正常パケットと DDoS パケットの要求発生パターンの違いを検知するのが困難になり，検知率が低下している．

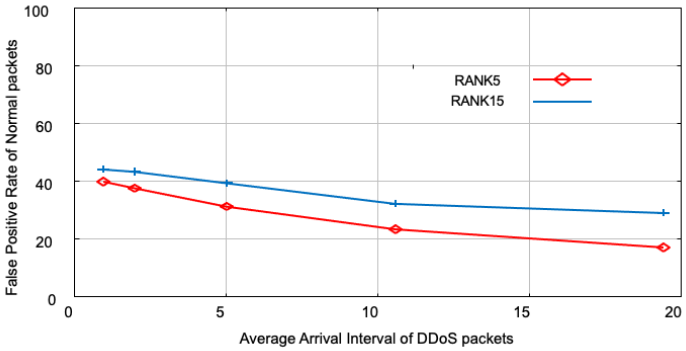

図 5.6: Z スコア法の閾値を変更したときの正常パケットの誤検知率

上図は RANK5 のコンテンツに対して，$\eta = 1.0$ と $\eta = 0.5$ で Z スコア法を適応し検知をおこなった際の正常パケットの誤検知率を示している．DDoS パケットの検知率と比較すると，性能評価で予想していたのと同様に，DDoS パケットを多く検知できている反面，正常パケットの誤検知も増えてしまっている．しかし，DDoS パケットの検知率の向上に対し，正常パケットの誤検知も増加は小さく，また正常パケットの誤検知は DNS

のログの確認により誤って棄却する危険性がないため $\eta = 0.5$ の方が良い結果であるといえる．

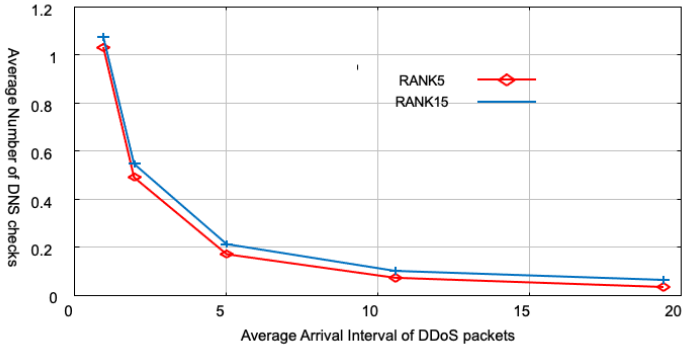

図 5.7: DNS の単位時間当たりの平均検査回数

上図は RANK5 のコンテンツに対して，$\eta = 1.0$ と $\eta = 0.5$ で Z スコア法を適応し検知をおこなった際の DNS の単位時間当たりの平均検査回数を示している．正常パケットの誤検知で評価したのと同様に，正常パケットの誤検知も増加は小さく，単位時間当たりの DNS の平均検査回数で見ると大きな差はない．

第6章　まとめ

本稿では，攻撃者が CDN の IP アドレスを発アドレスとして偽った場合にファイヤーウォールで検知不可能な問題に対し，二つのアプローチでの検知法を提案した．ファイヤーウォールで検知できない攻撃に対し，DNS の名前解決のログを確認することで検知を実施した．それは，CS からの正常な問い合わせの場合には，コンテンツ要求者の DNS サーバに名前解決のログが残るが，ボットからの OS の IP アドレスを直接用いた要求の場合，名前解決を用いないためログが残らないためである．しかし，全ての要求に対し攻撃の可能性を考慮し，DNS のログを確認すると OS の負荷が増大してしまう．本稿の目的としては，検知困難なこの様な攻撃に対し，DNS のログを活用し，OS の負荷を軽減しながら検知を行うことである．検知の際には，正常パケットと DDoS パケットの要求発生パターンの違いを活用し，到着間隔の差から危険性の判別を行っている．要求発生パターンの違いとは，CDN からオリジンサーバへの正常な配信要求はキャッシュミス時に発生するのに対し，DDoS 攻撃による配信要求は短い時間間隔で膨大な数が連続して発生するという違いを示している．本稿では，先行研究である到着間隔の差を設定した閾値によって要求の危険性の判別を行う二段階検知法に着目し，DNS の許容上限を満たす範囲での閾値の最大化を行い，最適な閾値を設定する二段階検知法の最適閾値設定法と到着間隔の逆数をデータとして外れ値を検知できる Z スコア法に適応することで検知を行う Z スコアによる DDoS 攻撃検知法の二つの提案方式を紹介した．

6.1　二段階検知法の最適閾値設定法

本方式は，先行研究である DDoS 攻撃の二段階検知法に着目し，方式に用いられる閾値を最適に設定するものである．最適な閾値とは，DNS の許容上限を満たす範囲での閾値の最大化を行うことである．それは，閾値 T を大きく設定しすぎた場合，DNS サーバでの問い合わせの有無を確認する回数が増え OS の負荷が増大する，一方閾値 T を小さく設定しすぎた場合，DDoS 攻撃を検知できない可能性があり，DDoS 攻撃に対しての強度が低下することを防ぐことを指している．このように閾値を最適に設

定することで，DNS サーバの処理能力上限を考慮しながら，DDoS 攻撃を最大限，検知することができる．性能評価では，閾値を仮に設定した際の特定のコンテンツにおける DNS の総検査レートから上限値を満たす最適な閾値 T を導出した．このグラフより，最適な閾値を求めることができる．

6.2　Z スコアによる DDoS 攻撃検知法

本方式では，外れ値を検知するアルゴリズムである Z スコア法を用いて DDoS 攻撃を検知を行った．到着間隔の差より Z スコア法で検知するため，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から到着間隔の逆数を Z スコア法に用いた．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った．攻撃の継続中は，正常な要求だけの時の要求の到着間隔パターンを学習するため，最初の攻撃検知後から終了まで 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，攻撃が終了したと判断した際に，平均値と標準偏差の更新を再開した．この様な手順により，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を行った．性能評価では，コンテンツを変更した場合と Z スコアの検知感度に関する閾値を変更した場合の 2 パターンにおいて行った．評価には，DDoS パケットの検知率と正常パケットの誤検知率を用いた．

6.2.1　コンテンツを変更したときの結果

人気度が低いコンテンツの方が正常パケットの到着間隔が大きいことにより検知しやすい結果が出た．しかし，人気度の低いコンテンツは，正常パケットを学習する際に大きい到着間隔で学習しているため，正常パケットを誤検知しやすくなっている．

6.2.2　Z スコア法の閾値を変更したときの結果

Z スコアの閾値を小さくし，感度を上げると，DDoS パケットを多く検知できている反面，正常パケットの誤検知も増えてしまっている．しかし，DDoS パケットの検知率の向上に対し，正常パケットの誤検知も増加は小さく，また正常パケットの誤検知は DNS のログの確認により誤って棄却する危険性がないため適度に閾値を小さくした方が良い結果である．

謝辞

本研究を行うに当たり，ご指導を頂いた上山教授に感謝します．また日常，有益な議論をして頂いた研究室の皆様に感謝します．

参考文献

[1] Ryohei Miyazaki, and Noriaki Kamiyama ,"CDN のキャッシュサーバを騙った DDoS 攻撃の防御方式," 総合大会 2021.

[2] Yeonwoo Nam, Changkyu Lee, Shingak Kang, and Juyoung Park, "Synchronization among CDN edge severs using P2P networking," 2015 International Conference on Information and Communication Technology Convergence (ICTC).

[3] Mohammed A. Saleh, and Azizah Abdul Manaf, "Optimal specifications for a protective framework against HTTP-based DoS and DDoS attacks," 2014 International Symposium on Biometrics and Security Technologies (ISBAST).

[4] J. v. Brakel, "Robust peak detection algorithm using z-scores," 2014.