エントロピーを用いた Slow HTTP DoS Attack 検知に関する研究

A STUDY ON DETECTION MTHOD OF SLOW HTTP DoS ATTACK USING ENTROPY

柴山光歩
Mitsumu SHIBAYAMA
指導教員　金井敦

法政大学大学院理工学研究科応用情報工学専攻修士課程

Slow HTTP DoS Attack, a type of low-bandwidth DoS attack, is a threat to services because it requires less resources for the attacker and is harder to be detected than conventional DoS attacks. In this paper, we show the feasibility of an attack detection method based on the entropy of the data arrival interval to the server and its average value. From the results of the verification of the proposed method, it is shown that it is possible to separate the normal state and the attack state in the experimental environment by setting threshold values for the two types of measured parameters, We also show that by narrowing the upper limit of the arrival interval of the acquired data, it is possible to separate the normal state from the attack state even when the ratio of attacks is reduced.

***Key Words** : Slow HTTP DoS Attack, Entropy, DoS, DoS Detection*

１．はじめに

インターネット上でのサービス不能攻撃(Denial of Service Attack，以下 DoS 攻撃)や分散型サービス不能攻撃(Distributed Denial of Service Attack，以下 DDoS 攻撃)は標的としたサービスを提供するサーバのリソースを枯渇させ，サービスの可用性を失わせることを目的とした攻撃であり[1]，さまざまな環境へ影響を与えている[2]．サービスを利用不可能にする方法として，ボットネット[1]を利用してサービス側の脆弱性をつく方法などが存在している．2022 年の第一四半期の調査[3]では特に OSI 参照モデルにおけるアプリケーション層を標的とした DoS 攻撃は前年同期比 164%増，前四半期比 135%増となっており被害は深刻化している．アプリケーション層を標的とした DoS 攻撃は HTTP プロトコルをはじめ DNS，SMTP など複数のプロトコルに悪用可能[4][5][6]であり，表向きは正当な通信として攻撃を実行しているためサービス側の攻撃検知を困難にする可能性がある．HTTP プロトコルを利用した DoS 攻撃の中に Slow HTTP DoS Attack[7]といわれる手法が存在している．この攻撃は通常の DoS 攻撃と比較して攻撃を行うトラフィック量を減少させ，帯域幅を抑える特徴をもっている．

複数の Web サーバが Slow HTTP DoS Attack に対し脆弱性をもっている[8]．このことからこの手法を用いた攻撃への対策が必要であると考えられる．攻撃の特性上 Slow HTTP DoS Attack の送信者がデータの送信間隔を意図的に操作するという点を利用し，現在サーバに対して送信されているデータからサーバへのデータの到着間隔のエントロピーを計測することで攻撃の判別を行う提案手法を用いて，実験環境における提案手法の検証を行う．

２．Slow HTTP DoS Attack

(１) DoS 攻撃

DoS 攻撃は，対象に対して大量のまたは不正なトラフィックを発生させることで対象となるサービスを利用不可能にすることを目的とした攻撃である．OSI 参照モデルにおいてどの層を標的にするかによって攻撃の種類が分けられる．従来の攻撃では OSI 参照モデルの第 3，第 4 層であるネットワーク層，トランスポート層を標的にしており攻撃対象のサーバのリソースを圧迫することを目的として大量のデータを送信する．大量のトラフィックを発生させる DoS 攻撃の例として，TCP セッションのハンドシェイクを利用する手法が存在する．この手法では悪意をもったクライアントがサーバに対して TCP コネクションを確立する際にクライアントから SYN パケットを送信し，サーバからの返答となる SYN-ACK パケットを無視し再度 SYN パケットを送信し続けることでサーバ側のメモリを枯渇させる[9]．もう 1 つの手法としては 7 層目にあたるアプリケーション層を標的とした DoS 攻撃が存在し，この手法では前述の攻撃のように通信量を増幅させる他にサーバが処理できないようなリクエストを送信することで対象サーバを利用不可能にする方法もある．従来のような通信量を増幅させる攻撃は，サーバに対する通信量や，送信元の IP アドレスやポートなどのフロー情報に基づいたエントロピーを計測する[10]ことで攻撃の進行を検知可能である．しかしアプリケーション層を標的とした DoS 攻撃には，対象となるアプリケー

ションの脆弱性をつくことで従来の DoS 攻撃よりも少ない帯域でサービスを利用不可能にする手法もあり，そのような手法の 1 つに Slow HTTP DoS Attack という攻撃が在する．

（2）Slow HTTP DoS Attack

Slow HTTP DoS Attack とは通常の DoS 攻撃と異なり，サーバと通信する際に悪意のあるクライアントがデータの送信および受信を遅延させることでセッションの継続時間を長引かせる．通信を長引かせることでサーバの許容する同時接続数を枯渇させ，サービスを利用不可能にさせる攻撃手法となっている．本論文で扱う Slow HTTP DoS Attack について以下の 3 種類に分類する．

a) Slow HTTP Headers Attack

Slow HTTP Headers Attack は，HTTP プロトコルで実装されている GET メソッドを用いた攻撃手法となっている．悪意を持ったクライアントがサーバに対し待機時間を挟 みながら長大なリクエストヘッダを送信し続けることで通信時間を長引かせる攻撃手法となっている．

b) Slow HTTP Body Attack

Slow HTTP Body Attack は，HTTP プロトコルで実装されている POST メソッドを用いた攻撃手法となっている．悪意をもったクライアントがサーバに対し待機時間を挟みながら長大なリクエストボディを送信し続けることで通信時間を長引かせる攻撃手法となっている．

c) Slow Read DoS Attack

Slow Read DoS Attack は HTTP プロトコルで実装されている GET メソッドを用いた攻撃であり，クライアントがサーバに対してなるべく小さい TCP ウィンドウサイズを指定することで，サーバからのデータの受け取りを遅延させることで通信時間を長引かせる．

３．関連研究

このような Slow HTTP DoS Attack を検知するための研究が複数存在している．その中の 1 つではネットワーク中のフローレコード中のフロー情報[11]に複数の機械学習を適用させて，セッションが通常のものであるか攻撃のものであるかを分類する手法を提案している[12][13]．フローレコードを用いてサーバに対する各セッションから複数の特徴を抽出することで分類を行なっている．これらの研究はそれぞれ特定の種類の攻撃のみを対象として分類を行なっている．また Slow HTTP DoS Attack を検知する方法として，1 つのセッションから複数の時間パラメータを計測し，その時間を閾値として攻撃が行われ ているかの判定を行う手法が存在している[14]．この研究では本論文で述べた 3 つの種類の攻撃に対応可能であるが，1 つのセッションごとに 5 つ分のパラメータを個別に計測する必要がある．これらのことを踏まえて，本論文では従来の手法よりも少ない特徴量で複数の攻撃手法に対応可能な検知方法を提案する．

４．提案手法

(1) 提案手法の概要

Slow HTTP DoS Attack の特徴として，悪意をもったクライアントがサーバに対し送信するデータの送信間隔を意図的に操作しているという点が挙げられる．攻撃の目的としてセッションの継続時間を長引かせるためにデータの送信間隔を操作していることから，分割された状態のトランスポート層のデータの受信間隔を計測すると Slow HTTP DoS Attack が行われていた場合は通常時よりも受信間隔が大きくなると考えられる．以上のことから通常の HTTP セッションと攻撃時の HTTP セッションのデータの送信の仕方の相違に着目し，その違いを数値化することで攻撃の進行中であるかの判定を行う手法を提案する．

(2) 使用する特徴量

平常時と攻撃時におけるデータの送信の仕方の違いを数値化するための特徴量を設定する．

Slow HTTP DoS Attack の特性から，攻撃進行時にデータの送信間隔が意図的に操作されており，その送信間隔には偏りが生じると仮定する．そこで送信の仕方の違いを数値化する特徴量としてエントロピーを用いることで，送信間隔の偏りによる数値の低下が観測できると考えられる．

また攻撃を行う際は攻撃者となるクライアントが待機時間を挟みながらデータを送信するため，到着間隔は平常時より長くなっていると仮定する．そこでエントロピーに加え，サーバ側へのデータの到着間隔の平均値を特徴量として攻撃の判定を行う．

(3) 提案手法におけるエントロピーの定義

エントロピーを計測するため，サーバ側にデータが到達してから次のデータが到着するまでの時間を計測する．全ての時間区間の中で，どの区間に収まったのかの確率を求めることでデータの到着間隔のエントロピーを算出する．サーバ側へのデータの到着間隔については，区切った間隔の総数をn, 1 つの間隔をΔt(s)として定義する.時間間隔の総数nの中で，到着間隔が$(k-1)\Delta t$秒より大きいかつ$k\Delta t$秒以下となるk番目の区間に収まる確率$p(k)$は式 1 のようになる．また提案手法で用いるサーバへのデータの到着間隔のエントロピーEを式 2 に示す．
図 1 にエントロピー計測の例を示す．

$$p(k) = \frac{K}{N} \tag{1}$$

Nは取得した時間間隔の総数，Kはk番目の時間間隔に収まった個数を示す．

$$E = -\sum_{k=1}^{n} p(k) log_2 p(k) \tag{2}$$

有限の時間区間の総数nおよびΔtを決定し，それぞれの区間kに収まる確率$p(k)$から平常時および攻撃時の平均情報量を求める．

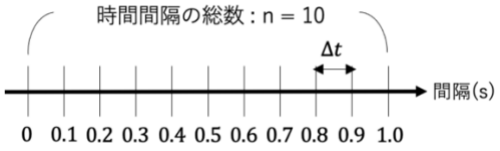

図 1 エントロピー計測の例($n = 10, \Delta t = 0.10$)

5．検証

(1) 実験環境

実験環境において web サーバへ正常な通信および攻撃の 通信を発生させ，実際に取得したデータからエントロピー値の算出などの分析を行うことで提案手法の検証を行う．実験環境を図 2 に示す．標的となる Web サーバを導入した仮想マシン，正常な通信を行う仮想マシン，Slow HTTP DoS Attack を行う 3 つの仮想マシンを導入して検証を行う．また攻撃のセッションを発生させるツールとして，本論文で対象とした 3 種類の攻撃が可能である slowhttptest を用いる．検証では標的となるサーバにおいて，クライアントからサーバへ送信されるトランスポート層のデータの取得を行うにあたり，全てのパターンにおいて 5 割以上のデータを採用する場合(データの到着間隔dが式 3 のようになる場合)と 9 割のデータを採用する場合(式 4)の 2 通りで検証を行う．

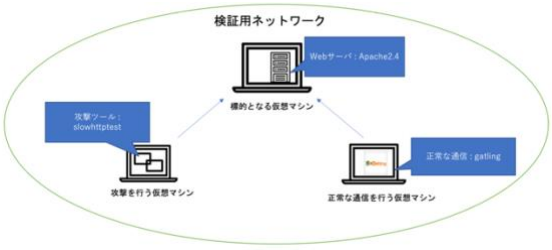

図 2 実験環境の構成

$$0 < d < 0.010 \quad (3)$$

$$0 < d < 1.0 \quad (4)$$

(2) 検証の条件とセッションの設定

検証の条件として平常時は通常の通信のみを発生させる．攻撃時は Slow HTTP DoS Attack と通常の通信を同時に発生させ各パターンについて 1 秒あたりに発生させるセッション数を変更して検証する．攻撃でない通常の HTTP セッションは 1 秒当たり 1 件，2 件，3 件，4 件の 4 通りで検証を行う．また攻撃のセッションは全ての場合において 1 秒当たり 5 件の割合で発生させる．正規のユーザが単一のリクエストのみでなく複数の操作を連続して行うことを想定し，通常のセッションでは 1 つのセッション内で 3 件の HTTP リクエストを，待機時間を挟みながら実行させる．攻撃にあたるセッションでは，1 つのセッション内で 1 件の HTTP リクエストを実行させる．データの到着間隔の計測において，取得するデータの範囲を式 4 で設定した場合の到着間隔のエントロピーを式 5 で，式 3 で行った場合の到着間隔のエントロピーを式 6 で定義する．

$$E = -\sum_{k=1}^{n} p(k) log_2 p(k) \ (n = 100, \Delta t = 1.0 \times 10^{-4}) \ (5)$$

$$E = -\sum_{k=1}^{n} p(k) log_2 p(k) \ (n = 10000, \Delta t = 1.0 \times 10^{-4}) \ (6)$$

6．測定結果

検証を行なった際のサーバへ送信されるデータの到着間隔のエントロピーと到着間隔の平均値を示す．

(1) 攻撃時のエントロピーの分布

平常時と攻撃実行時の状況の差について検証するため，平常時および Slow HTTP DoS Attack 実行時のエントロピーの計測を行う．この項では攻撃時は攻撃の通信のみを発生させている．それぞれのパターンにおけるエントロピーの値を表 1 に，到着間隔の秒単位での平均値を表 2 に示す．また Headers Attack のエントロピーの分布を図 3，Body Attack の分布を図 4，Read DoS Attack の分布を図 5 に示す．グラフの横軸はパケットの到着間隔の区間，縦軸はそれぞれの区間に収まる確率を，グラフ中の青色の分布は平常時，オレンジ色の分布は攻撃実行時の状態を示している．またこの検証においては平常時，攻撃時共にセッション数を 1 秒あたり 5 件ずつ発生させている．結果およびグラフから攻撃時は平常時よりエントロピーの値も下降傾向があることが分かる．またデータ取得の上限を 0.010 秒とした場合では攻撃時の方が到着間隔の平均値は低く，上限を 1.0 秒まで取った場合は逆に攻撃時の方が到着間隔の平均値は長くなっていることが分かる．

表 1 平常時と攻撃時のエントロピー値

パターン	エントロピー値
平常時(0.010s)	5.4544
Headers(0.010s)	2.4944
Body(0.010s)	1.5251
Read(0.010s)	3.0190
平常時(1.0s)	7.3162
Headers(1.0s)	4.6005
Body(1.0s)	2.8057
Read(1.0s)	5.9008

表 2 平常時と攻撃時の到着間隔の平均値

パターン	平均値(s)
平常時(0.010s)	0.004416
Headers(0.010s)	0.0002622
Body(0.010s)	0.0002814
Read(0.010s)	0.0007210
平常時(1.0s)	0.01414
Headers(1.0s)	0.06985
Body(1.0s)	0.01496
Read(1.0s)	0.04586

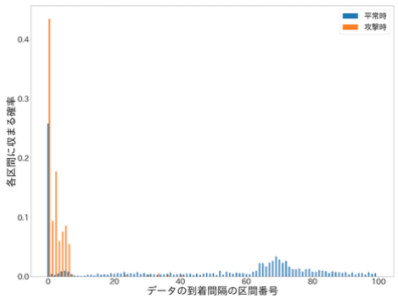

図 3　エントロピー分布:Headers(5/s)

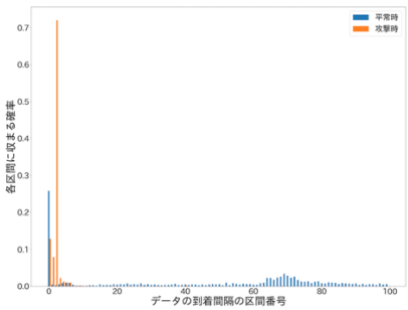

図 4 エントロピー分布:Body(5/s)

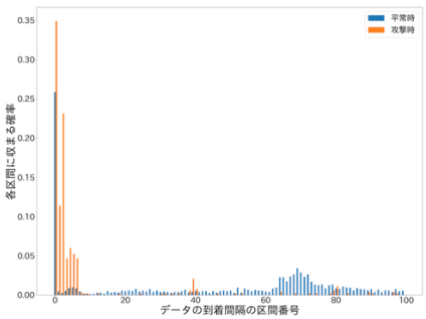

図 5 エントロピー分布:Read(5/s)

(2) 平常時、攻撃時のエントロピーと平均値

実際の状況では Slow HTTP DoS Attack の進行時においても通常の通信が並行してサーバ・クライアント間で行っていると想定される．この項では攻撃時に通常の通信も発生させた状態でデータを収集する．Headers Attack のエントロピー値の結果を表 3 に，データの到着間隔の平均値を表 4 に示す．Body Attack のエントロピー値の結果を表 5 に，データの到着間隔の平均値を表 6 に示す．Read DoS Attack のエントロピー値の結果を表 7 に，データの到着間隔の平均値を表 8 に示す．またそれぞれの攻撃について，平常の通信 4/s に対して攻撃の通信を 5/s で発生させた場合のエントロピーの分布を図 6，図 7，図 8 に示す．

表 3 エントロピー(平常時と Headers)

パターン	平常時	Headers
1/s(0.010s)	5.5156	4.4860
2/s(0.010s)	5.6084	5.2058
3/s(0.010s)	5.5880	5.3317
4/s(0.010s)	5.5323	5.4953
1/s(1.0s)	7.9633	7.1652
2/s(1.0s)	7.9256	7.2373
3/s(1.0s)	7.6073	7.1606
4/s(1.0s)	7.6950	7.4904

表 4 到着間隔の平均値(平常時と Headers)

パターン	平常時(s)	Headers(s)
1/s(0.010s)	0.005564	0.002450
2/s(0.010s)	0.005257	0.003326
3/s(0.010s)	0.004776	0.003543
4/s(0.010s)	0.004272	0.003594
1/s(1.0s)	0.04992	0.03330
2/s(1.0s)	0.03131	0.02238
3/s(1.0s)	0.02020	0.01667
4/s(1.0s)	0.01858	0.01471

表 5 エントロピー(平常時と Body)

パターン	平常時	Body
1/s(0.010s)	5.5156	2.3897
2/s(0.010s)	5.6084	3.1377
3/s(0.010s)	5.5880	3.9129
4/s(0.010s)	5.5323	3.9691
1/s(1.0s)	7.9633	4.1792
2/s(1.0s)	7.9256	4.7477
3/s(1.0s)	7.6073	5.2670
4/s(1.0s)	7.6950	5.4734

表 6 到着間隔の平均値(平常時と Body)

パターン	平常時(s)	Body(s)
1/s(0.010s)	0.005564	0.0008829
2/s(0.010s)	0.005257	0.001391
3/s(0.010s)	0.004776	0.001880
4/s(0.010s)	0.004272	0.001995
1/s(1.0s)	0.04992	0.01283
2/s(1.0s)	0.03131	0.01070
3/s(1.0s)	0.02020	0.008243
4/s(1.0s)	0.01858	0.008399

表 7 エントロピー(平常時と Read)

パターン	平常時	Read
1/s(0.010s)	5.5156	5.0373
2/s(0.010s)	5.6084	5.5314
3/s(0.010s)	5.5880	5.4801
4/s(0.010s)	5.5323	5.6317
1/s(1.0s)	7.9633	7.5054
2/s(1.0s)	7.9256	7.6767
3/s(1.0s)	7.6073	7.5184
4/s(1.0s)	7.6950	7.5006

表 8 到着間隔の平均値(平常時と Read)

パターン	平常時(s)	Read(s)
1/s(0.010s)	0.005564	0.003174
2/s(0.010s)	0.005257	0.003726
3/s(0.010s)	0.004776	0.003690
4/s(0.010s)	0.004272	0.003719
1/s(1.0s)	0.04992	0.02995
2/s(1.0s)	0.03131	0.01987
3/s(1.0s)	0.02020	0.01643
4/s(1.0s)	0.01858	0.01286

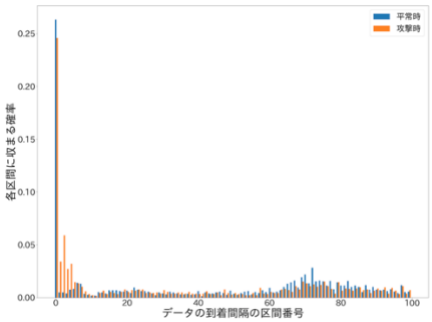

図 6 エントロピー分布(上限 0.010s, 4/s, Headers)

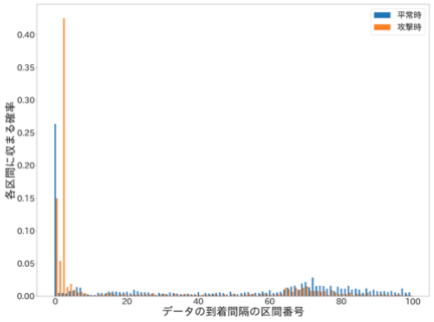

図 7 エントロピー分布(上限 0.010s, 4/s, Body)

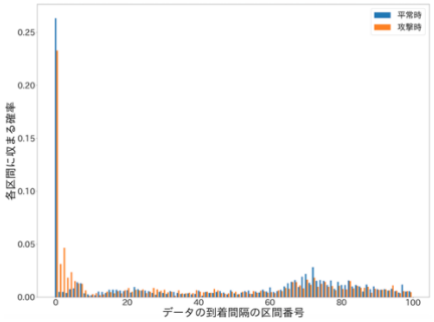

図 8 エントロピー分布(上限 0.010s, 4/s, Read)

(3) エントロピーと平均値の関係

平常時および攻撃実行時のパケット間隔のエントロピー値と平均値の関係について，データの取得範囲の上限を 0.010 秒までとした場合を図 9 に，1.0 秒までとした場合を図 10 に示す．グラフの横軸はパケットの到着間隔の平均値を表したもの，縦軸は各パターンにおけるエントロピーの値となっている．

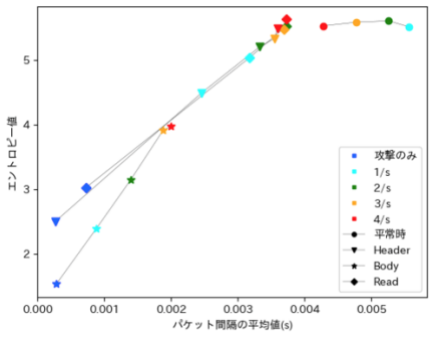

図 9 エントロピーと平均値の関係(上限 0.010s)

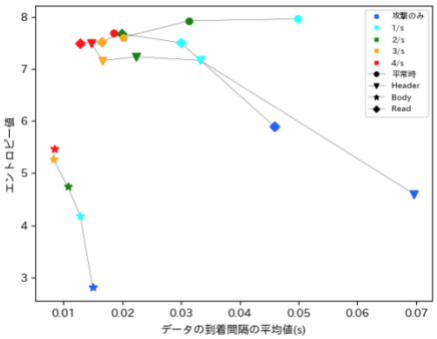

図 10 エントロピーと平均値の関係(上限 1.0s)

7．考察

データの取得範囲について 0.010 秒を上限とした場合では Headers Attack と Body Attack はどの場合においてもエントロピーおよび平均値は平常時を下回っている．また Read DoS Attack については 4/s 以外の場合ではエントロピーの値が平常時を下回っており，データの到着間隔の平均値はどの場合においても平常時を下回っている．このことから，Slow HTTP Headers Attack はエントロピー値 5.50 以下または到着間隔の平均値 0.0040 秒以下を閾値とすることで通常の通信 4/s 以下において分類可能であると考えられる．Slow HTTP Body Attack はエントロピー値 4.00 以下または到着間隔の平均値 0.0020 秒 以下を閾値として通常の通信 4/s 以下を分類可能であると 考えられる．Slow Read DoS Attack については，エントロピーの閾値を 5.50 以下で通常の通信 1/s において分類可能，また到着間隔の平均値 0.0040 秒以下を閾値とすることで通常の通信 4/s 以下において分類可能であると考えられる.データの取得範囲を 1.00 秒を上限とした場合では Headers Attack と Body Attack では，どのパターンにおいてもエントロピー値は平常時を下回っている．また Read DoS Attack については通常の通信 2/s 以外のパターンでは，攻撃時のエントロピー値は平常時を下回っている．このことから，Slow HTTP Headers Attack はエントロピー値 7.50 を閾値とすることで攻撃 5/s に対して通常の通信 4/s 以下において分類可能であり，また Slow HTTP Body Attack はエントロピー値 6.00 を閾値とすることで通常の通信 4/s 以下において分類可能であると考えられる．Slow Read DoS Attack についてはエントロピー値 7.60 を閾値とすることで通常の通信 2/s 以外で攻撃する場合以外で，またはデータの到着間隔 0.017 秒以下を閾値とすることで通常の通信 3/s 以上の場合で攻撃時と通常時の分類が可能であると考えられる．6 章(1)より，データの到着間隔のエントロピーについて，攻撃のみの場合の方が平常時よりも到着間隔が低くなっていた．これは正常な通信においては正規のユーザが操作することを考慮してセッション内で待機時間を挟みながらセッションを続行していたため，通常の通信の方がデータの到着が長引いていたことが原因として考えられる．到着間隔 0.0060 秒以上の区間に平常時のボリュームゾーンが存在し，6 の結果より正常な通信の割合を増加させると攻撃時と平常時のボリュームゾーンが重なることで，両者の差が縮まっていくと考えられる．この部分を取得するデータの範囲から外し，データの取得範囲の上限を 0.0010 秒以下で計測した際のエントロピーの定義を式 7 に，エントロピー値の結果を表 8，表 9，表 10 に，その平均値(秒)を表 11，表 12，表 13 に，エントロピーと平均値の結果を図 11 に示す．この状態ではエントロピー値 3.6 以下を閾値として攻撃時と平常時の分離が可能ではあるが平常状態のボリュームゾーンが常に 0.0060 秒以上であるとは限らず，この方法については引き続き検討が必要であると考えられる．

$$E = -\sum_{k=1}^{n} p(k) log_2 p(k) \ (n = 100, \Delta t = 1.0 \times 10^{-5}) \ (7)$$

表 8 エントロピー(平常時と Headers，上限 0.0010s)

パターン	平常時	Headers
5/s	2.7737	4.0675
10/s	3.1170	4.0071
15/s	3.4186	3.7885

表 9 エントロピー(平常時と Body，上限 0.0010s)

パターン	平常時	Body
5/s	2.7737	3.8140
10/s	3.1170	3.8943
15/s	3.4186	4.0763

表 10 エントロピー(平常時と Read，上限 0.0010s)

パターン	平常時	Read
5/s	2.7737	4.0355
10/s	3.1170	3.7838
15/s	3.4186	3.7017

表 11 平均値(平常時と Headers，上限 0.0010s)

パターン	平常時(s)	Headers(s)
5/s	0.00008616	0.0001464
10/s	0.00009732	0.0001340
15/s	0.0001031	0.0001230

表 12 平均値(平常時と Body，上限 0.0010s)

パターン	平常時(s)	Body(s)
5/s	0.00008616	0.0001963
10/s	0.00009732	0.0001596
15/s	0.0001031	0.0001586

表 13 平均値(平常時と Read, 上限 0.0010s)

パターン	平常時(s)	Read(s)
5/s	0.00008616	0.0001488
10/s	0.00009732	0.0001165
15/s	0.0001031	0.0001133

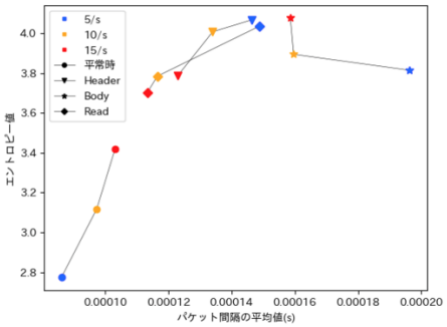

図 11 エントロピーと平均値の関係(上限 0.0010s)

8．おわりに

検証を通して Slow HTTP DoS Attack の種類に応じてデータの到着間隔のエントロピー値およびその平均値の閾値を設定することにより，平常時と攻撃実行時の分離が可能であることが分かった．また今回の検証は限られた実験環境内でのシミュレーションとなっていたため，今後の課題としてより実際の環境に近い形での検証，標的へのトラフィック量の違いによるエントロピー値などの違いも考慮した上で適切な閾値を決定していく必要がある．

謝辞

本研究を進めるにあたり様々な指導，ご鞭撻を賜りました．また金井敦教授，呉謙助教授をはじめ，本稿を作成するにあたりご協力いただいた皆様に深く感謝申し上げます．

参考文献

1) 寺田真敏：DoS/DDoS とは，情報処理学会誌, vol.54, No.5, pp.428-435(2013).

2) 齋藤衛：Dos/DDoS 攻撃対策(1) ～ISP における DDoS 対策の現状と課題～，情報処理学会誌, vol.54, No.5, pp.2046-2069(2013).

3) DDoS Attack Trends for Q1 2022, available from 〈https://radar.cloudflare.com/notebooks/ddos-2022-q1〉 (accessed 2022-08-20).

4) Marcin Nawrocki, Mattijs Jonker, Thomas C. Schmidt, Matthias W¨ahlisch: The Far Side of DNS Amplification: Tracing the DDoS Attack Ecosystem from the Internet Core, IMC '21: Proceedings of the 21st ACM Internet Measurement Conference, pp.419-434(2021).

5) Andrei-Daniel Tudosi, Doru Gabriel Balan, Alin Dan Potorac: New Snort rule for detection and prevention of SMTP e-mail bomb attacks, International Conference on Development and Application Systems, pp.78-84(2022).

6) Yingbo Li, Bo Sun, Lianzhong Liu, Yadong Wang: A Survey of defence mechanisms against application layer distributed denial of service attacks, International Conference on Software Engineering and Service Science, pp.1034-1037(2015).

7) Enrico Cambiaso, Gianluca Papaleo, Maurizio Aiello: Taxonomy of Slow DoS Attacks to Web Applications, Recent Trends in Computer Networks and Distributed Systems Security, pp.195-204(2012).

8) Nikhil Tripathi: How Secure are Web Servers? An Empirical Study of Slow HTTP DoS Attacks and Detection, International Conference on Availability, Reliability and Security, pp.454-463(2016).

9) Mr. Hrishikesh Shriram Salunkhe, Prof. Sanjay Jadhav, Prof. Vijay Bhosale: Analysis and Review of TCP SYN Flood Attack on Network with Its Detection and Performance Metrics, IJERT, 2017, vol.6, issue 01, pp.250-256, available from 〈https://www.ijert.org/research/analysis-and-review-of-tcp-syn-flood-attack-on-network-with-its-detection-and-performance-metrics-IJERTV6IS010218.pdf〉 (accessed 2023-01-30).

10) G. Nychis, V. Sekar, D. G. Andersen, H. Kim, and H. Zhang: An empirical evaluation of entropy-based traffic anomaly detection, Proceedings of the 8th ACM SIGCOMM conference on Internet measurement, pp.151-156(2008).

11) RFC 7011 - Specification of the IP Flow Information Export (IP- FIX) Protocol for the Exchange of Flow Information, available from 〈https://datatracker.ietf.org/doc/html/rfc7011〉(accessed 2023-01-30).

12) Cnad Calvert, Clifford Kemp, Taghi M. Khoshogoftaar, Maryam M. Najafabadi: Detecting Slow HTTP POST Attacks Using Netflow Features, 32nd FLAIRS Conference, pp.387-390(2019).

13) Clifford Kemp: Utilizing Netflow Data to Detect SLow Read Attacks, 2018 IEEE International Conference on Information Reuse and Integration, pp.108-116(2018).

14) Enrico Cambiaso, Maurizio Aiello, Maurizio Mongelli, Ivan Vaccari: Detection and classification of Slow DoS Attacks targeting network servers, Proceedings of the International Conference on Availability, Reliability and Security, pp.1- 7(2020).