ハイブリッド型SYN Flood防御手法の提案とその性能評価に関する研究

片野田 拓望[1]　岡村 耕二[1]

概要：Dos 攻撃の一種である SYN Flood 攻撃は，TCP の SYN パケットを大量に送信することでサーバーのリソースを消費させて正規の接続を妨害する攻撃であり，その防御・緩和手法について研究が進められている．その中でもサーバーとクライアント間の中継機器上で動作するネットワークベースの防御手法は，サーバーの負荷軽減や帯域保護の観点で有効であるが，フィルタの精度や負荷・遅延の観点で課題を有している．本研究では，ネットワークベースの既存手法である TCP Intercept と SYN Drop を組み合わせて用いることでより効果的な防御が可能である見込みを得ている．本発表では既存手法と提案手法の比較検証を行い，負荷や防御可能な攻撃について示す．

キーワード：DoS 攻撃，SYN Flood 攻撃，ネットワークセキュリティ

Study on SYN Flood Defense Method Using Hybrid Approach

Abstract: The SYN Flood attack, a type of Dos attack, is an attack that sends a large number of TCP SYN packets to consume server resources and disrupt legitimate connections. Among defense methods, network-based methods that operate on relay devices between servers and clients are effective in terms of server load reduction and bandwidth protection, but they have issues in terms of filter accuracy, load, and latency. In this study, we have found that a combination of TCP Intercept and SYN Drop, which are existing network-based methods, can provide more effective protection. In this presentation, we compare and verify the existing and proposed methods, and show the amount of load and defensible attacks.

Keywords: Denial-of-Service attack，TCP SYN Flood attack，Network Security

1. はじめに

近年，インターネットの急速な普及とデジタル化の進展に伴い，サイバーセキュリティの重要性が一層高まっている．特に，サービス拒否（Denial of Service, DoS）攻撃は，国家や企業・組織のネットワークインフラを標的とした攻撃として，深刻な問題になっている．その中でも，SYN Flood 攻撃は広く用いられている古典的な攻撃手法の一つであり，依然として多くの攻撃者によって悪用されている．Kaspersky 社の調査によると，2022 年第三半期の DDoS 攻撃のうち SYN Flood 攻撃は全体の 26.96%を占めており，2 番目に多い攻撃タイプとなっている [1].

SYN Flood 攻撃は，TCP プロトコルの 3 ウェイハンドシェイクにおける脆弱性を悪用したもので，SYN パケットを大量に送信し，接続要求を半永久的に維持させることにより，サーバーのリソースを消費させて正規の接続を妨害する．この攻撃は非常にシンプルであるため攻撃コストが低い一方で，防御側は受信した SYN パケットの情報のみでは正常なパケットと攻撃パケットを区別するのが困難であるという課題を有しており，効果的な防御・緩和手法が求められている．

防御・緩和のアプローチのひとつであるネットワークベースの防御手法は，ルーターやプロキシ・ファイアウォール等の中継装置を用いて，サーバーとクライアントの間で防御を行う．攻撃パケットがサーバーに到達するより前に防御を行うことができるため，サーバーの負荷軽減や帯域保護の観点から有効である [2] 一方，中継装置に大きな負荷がかかるという課題を有している [3], [4].

[1] 九州大学大学院 システム情報科学府
Kyushu University Graduate School of Information Science and Electrical Engineering

ネットワークベースの既存手法において，各手法は特定の場面においては有効であるもののそれぞれ課題を有しており，それらの改善が求められている．また，関連研究では負荷や遅延，認証の脆弱性などの可能性が示唆されていたものの，その検証は十分ではない．特に攻撃による負荷・遅延への影響は，サーバーやネットワーク機器のリソース・構成などの実験環境によって大きく変化するため，同一環境下で比較検証を行う必要がある．

本研究では，ネットワークベースの既存手法である TCP Intercept と SYN Drop を組み合わせたハイブリッド型の防御手法を提案し，提案手法と既存手法の比較を行うことで，提案手法の有効性について検証・考察を行った．具体的には，既存手法と提案手法のアルゴリズムについて，負荷，認証の強度，遅延の観点から検討し，その後それぞれのアルゴリズムをブリッジに実装して比較実験を行うことでその有効性について考察した．

2. SYN Flood 攻撃の概要

本章では，まず DoS 攻撃の分類について触れたのち，TCP 通信の 3 ウェイハンドシェイクの仕組みと，それを悪用した SYN Flood 攻撃の概要について述べる．

2.1 Dos・DDoS 攻撃の分類

DoS 攻撃は，ターゲットとなるシステムやネットワーク，サービスが正常に機能しなくなるように意図的にリソースを消費させたり，システムの処理能力を超過させたりする攻撃のことである．その攻撃手法は多岐にわたっており，防御を検討する際にはそれぞれの特徴を理解することが不可欠である．関連研究 [3] では，特に分散型の攻撃である DDoS 攻撃を，プロトコルの観点からネットワーク/トランスポート層の flooding 攻撃とアプリケーション層の flooding 攻撃に分類している．

2.1.1 アプリケーション層の flooding 攻撃

アプリケーション層の flooding 攻撃は L7(Layer7) DDoS 攻撃とも呼ばれ，DNS や HTTP 等を用いた特定のアプリケーションを攻撃対象とする．サーバーに負荷を与えることで正規のユーザーのサービス利用を妨害するが，DNS のランダムサブドメイン攻撃のように大量のトラフィックを送信する攻撃だけではなく，Slowloris 攻撃のように長い時間をかけて攻撃することでサーバーのリソースを消費させるものなど，アプリケーションに応じてその攻撃特性は多岐にわたる．

2.1.2 ネットワーク/トランスポート層の flooding 攻撃

ネットワーク/トランスポート層の flooding 攻撃は，ICMP や TCP,UDP などのパケットを大量に送信することで，サーバーのリソースや通信帯域などを消費させる．アプリケーション層の flooding 攻撃と比べて特定のサービスに依存しにくいため，攻撃の汎用性が高いことが特徴である．代表的なものとして，UDP Flood 攻撃や smurf 攻撃，SYN Flood 攻撃が挙げられる．

本研究では特に TCP の仕様を悪用した攻撃である SYN Flood 攻撃に焦点を当て，その防御手法について検討する．

2.2 3 ウェイハンドシェイク

TCP 通信は，はじめにクライアントとサーバーで 3 ウェイハンドシェイクを行いコネクションを確立することで，信頼性の高い通信を実現している．3 ウェイハンドシェイクは以下の手順で行われる．

1. サーバーがクライアントから SYN パケットを受信すると，カーネルはその情報を Transmission Control Block (TCB) というデータ構造で syn backlog に保持する [5].
2. サーバーが SYN-ACK パケットにシーケンス番号をセットし，クライアントに返送する．
3. クライアントが SYN-ACK パケットを受信し，シーケンス番号に従って適切な ACK パケットをサーバーに返送する．
4. サーバーは ACK パケットを受信すると，syn backlog から該当の TCB を削除し，3 ウェイハンドシェイクを完了してデータ転送を行う．

syn backlog が満杯のときに新たな SYN パケットを受信すると，その接続要求は無視されるか，syn backlog 内の古い TCB が削除される．

2.3 SYN Flood 攻撃

SYN Flood 攻撃では，攻撃者は対象サーバーに大量の SYN パケットを送信し，対象サーバーからの SYN-ACK パケットに意図的に応答しない．すると，サーバーの syn backlog は 3 ウェイハンドシェイクが完了していない half open 状態の接続で飽和し，新規の接続が困難になる．攻撃の SYN パケット自体に悪意のあるペイロードが含まれているわけではなく，また攻撃者は SYN パケットの送信元 IP アドレスをランダムに偽装して攻撃を行うことも可能であるため，SYN パケットの情報単体では正規のパケットと攻撃パケットを区別することは困難である．

3. 防御・緩和手法

近年の OS は大きなサイズ syn backlog を有しているが，SYN Flood 攻撃の攻撃コストの低さから，特に分散型の攻撃に対しては十分に対応できない．そのため，適切な防御・緩和手法を設計する必要がある．本研究では防御手法のアプローチを，対象サーバー上で実行されるサーバーベースと，ネットワーク上の中継装置上で動作するネットワークベースに分類し，主にネットワークベースの防御手法について議論する．

3.1 サーバーベース

サーバーベースの防御手法は，対象サーバー上のカーネルやソフトウェアとして動作する．例えば，SYN cookies[7] や SYN cache[6] はサーバーのカーネルで動作する機能の一つである．

3.1.1 SYN cookies

SYN cookies は，syn backlog にクライアントのデータを保持することなくコネクションを確立する機能である．サーバーが SYN パケットを受信すると，カーネルはその情報をハッシュ化したものをマジックナンバーとして SYN-ACK パケットのシーケンス番号にセットし返送する．それに対してクライアントから ACK パケットが返ってくると，カーネルはクライアントの情報からマジックナンバーを再計算し，ACK パケットから得られたマジックナンバーが一致しているかを確かめることでクライアントの正当性を検証し，コネクションを確立する．この手法により syn backlog の飽和を防ぐことができるが，マジックナンバーの生成でサーバーに大きな負荷を与える可能性がある．

3.1.2 SYN cache

SYN cache は，TCB よりも軽いデータ構造を用いてそれをキャッシュとして保持する．これにより，より多くの接続要求に対応できるようになる一方で，キャッシュがあふれるほどの規模の攻撃に対しては対応できない可能性があり，根本的な解決にはなっていない．

3.2 ネットワークベース

サーバーベースの防御手法は SYN Flood 攻撃に対して一定の効果があるものの，大量の攻撃パケットすべてに対して適用するとそれ自体がサーバーへの負荷となり，余分なリソースを消費する場合がある．

それに対して，ネットワークベースの防御手法は，攻撃パケットが対象サーバーに到達する前に防御できるため，サーバーの負荷軽減が期待できるほか，サーバーの OS に依らない点や帯域保護の観点からも有効である．関連研究では，以下のような複数のアプローチが検討されている．

3.2.1 ingress filtering

ingress filtering[3] は，攻撃トラフィックを送信元のエッジでブロックするアイデアである．具体的な防御手法としては，送信元 IP アドレスの検証がある．現在の IP プロトコルでは送信元の IP アドレスの検証はされないため，送信元 IP アドレスを偽装して送信することが可能である．通常の通信では，サーバーからの通信が正常にルーティングされなくなるため送信元 IP アドレスを偽装した状態で通信はできないが，SYN flood 攻撃や smurf 攻撃では偽装していても攻撃が成立する．そこで，ingress filtering は，送信元のエッジのルーターが IP パケットを受信したときに，その IP アドレスが内部ネットワークに存在する有効なものかを検証し，不正であればドロップする．

ingress filtering を実装したルーターのネットワーク内から送信元 IP アドレスを偽装した攻撃を行った場合は効果が期待できる反面，現実的に有効に防御をするにはこの機能が多くのルーターで広く展開されている必要がある．また，ルーターのネットワーク内に存在する有効な送信元 IP アドレスに偽装した場合は検出されない．

3.2.2 TCP Intercept

TCP Intercept[2], [8] は，中継装置がサーバーの代理で 3 ウェイハンドシェイクを行い，クライアントの IP アドレスを認証する手法である．未認証の送信元 IP アドレスから SYN パケットを受信したとき，中継装置がサーバーの代理で SYN-ACK パケットを返送し，クライアントからの ACK パケットを受信したら正規のクライアントとみなしてその IP アドレスを認証する (図 1)．これにより，攻撃パケットは対象サーバーに到達できず，正規のクライアントのみが接続を確立することができる．SYN Flood 攻撃は意図的に 3 ウェイハンドシェイクを完了しない攻撃であるため，TCP Intercept による認証をバイパスすることは困難である．一方で，大量の攻撃 SYN パケット全てに代理応答を行うことで中継装置に負荷がかかることが懸念される．

また，中継装置はクライアントとの 3 ウェイハンドシェイクを完了したのちにサーバー側とも 3 ウェイハンドシェイクを行いコネクションを確立するため，初回接続時にはその分の遅延が発生する．

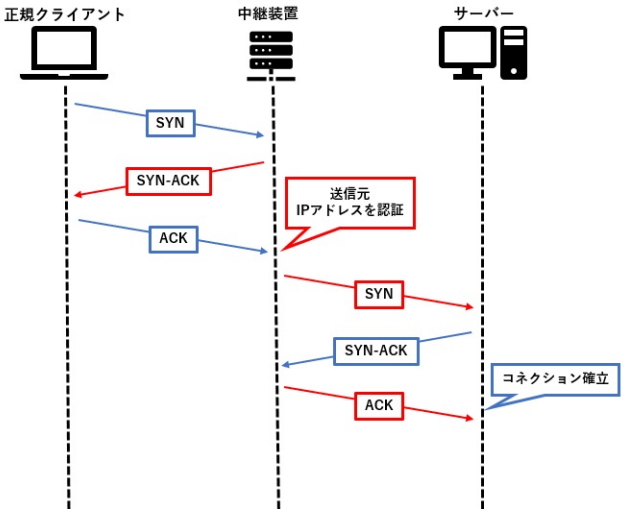

図 1 TCP Intercept の処理フロー

3.2.3 SYN Drop

SYN Drop[8] は，それぞれの IP アドレスから送信された最初の SYN パケットを意図的にドロップし，クライアントに再送を促す手法である．TCP 通信では，送信したパケットに対して一定時間 ACK パケットの返答がない場合は，カーネルが該当のパケットを再送する．そのため，

SYN Drop により最初の SYN パケットがドロップされた場合も，クライアントのカーネルにより一定時間後に SYN パケットが再送され，それが認証されることで正常にコネクションを確立できる（図 2）．一方 SYN Flood 攻撃では通常，再送制御は行われないため，攻撃パケットは対象サーバーに到達することなくドロップされる．

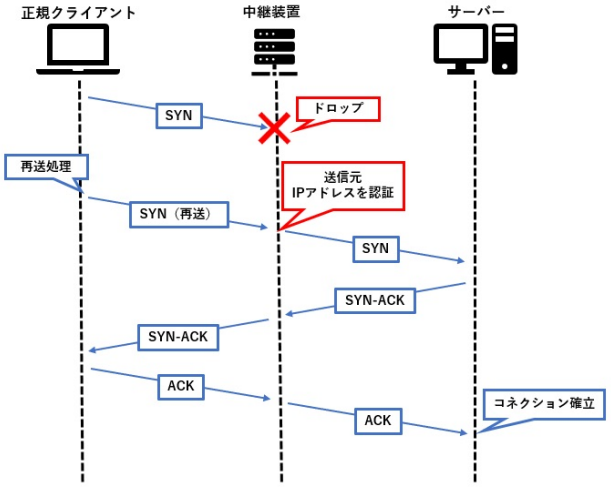

図 2 SYN Drop の処理フロー

TCP Intercept と比較したとき，SYN Drop は代理応答に伴うパケットの生成や送信などの複雑な処理を必要としないため，高速かつ低負荷であることが見込まれる．関連研究 [8] ではそれが示唆されているもののその検証は十分ではなく，5 章では実際に実験を行うことで負荷の比較検証を行う．

また、認証の強度の観点では、攻撃者は同じ IP アドレスの SYN パケットを二重で送信することで再送を偽装し，防御をバイパスできる可能性がある（図 3）．

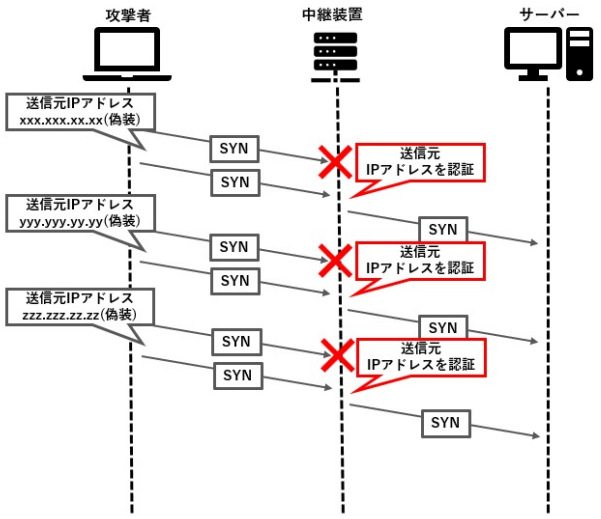

図 3 SYN Drop の認証をバイパスし得る攻撃シナリオ

また，送信した SYN パケットに対してサーバーから返信がない場合，カーネルは既定の時間で再送制御を行う．クライアントが初回接続時に SYN Drop による認証を受けてサーバーに接続する場合にはその時間が遅延となる．

3.2.4 課題

上記のネットワークベースのアプローチは，中継装置の負荷が増大してしまう可能性や，攻撃パケットの検証の精度が不十分で高度な攻撃に対応できない可能性を孕んでおり，それらを十分に検証する必要がある．

4. 提案手法

本章では，既存手法である TCP Intercept と SYN Drop を組み合わせたハイブリッド型の防御手法を提案し，TCP Intercept の強固な認証と SYN Drop の低負荷な処理の両立を試みる手法について説明を行う．

4.1 提案手法のアイデア

TCP Intercept は，SYN パケットの送信元 IP アドレスに対して強固な認証を行うことで堅牢な防御を実現する一方．大量の攻撃 SYN パケット全てに代理応答を行うとそれにより中継装置の負荷が増大する可能性がある．対して SYN Drop は，TCP Intercept と比較してシンプルな処理であるため低負荷で防御できることが示唆されているが [8]，認証がの強度が低いため，防御がバイパスされ攻撃パケットがサーバーに到達してしまう可能性がある．

そこで提案手法では，これら二つの手法を組み合わせて用い，低負荷かつ堅牢な防御の実現を試みる．具体的なフローは図 4 のようになる．中継装置が新規の送信元 IP アドレスから SYN パケットを受信したとき，まずはそれを SYN Drop のアイデアでドロップし再送を促す．そして再送されてきた二度目の SYN パケットに対して TCP Intercept のアイデアで代理応答を行い，クライアントが正常に 3 ウェイハンドシェイクを完了したら送信元 IP アドレスを認証し，サーバーにコネクションを渡す．

これにより，攻撃の大半は SYN Drop の軽量な処理で防御し，それをバイパスした高度な攻撃のみに TCP Intercept による強固なセッション管理を適用できるため，SYN Drop の処理の軽量さと TCP Intercept の認証の強度を両立した防御を期待できる．

4.2 提案手法の有効性

提案手法の有効性について，負荷と認証の強度の観点から述べる．負荷は TCP Intercept と比較し，認証の強度は SYN Drop と比較することで，両既存手法の課題を解決できているかを議論する．

4.2.1 負荷

提案手法は，SYN Drop の防御を先に行うことで高負荷な TCP Intercept による防御を最小限に抑えるというアイデアに基づいている．そこで，提案手法が攻撃トラフィッ

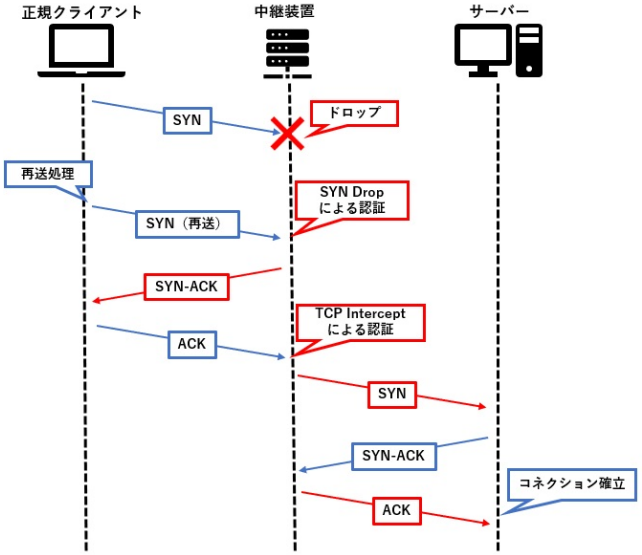

図 4 提案手法の処理フロー

クを処理した際にどの程度 TCP Intercept による処理を減らすことができるのかについて，以下のように定式化する．

$$N_T = P - U \tag{1}$$

N_T　TCP Intercept による認証を適用する攻撃 SYN パケットの個数（個）
P　攻撃 SYN パケットの総数（個）
U　攻撃 SYN パケットの総数 N のうち，送信元 IP アドレスがユニークであるものの個数（個）

多くの SYN Flood 攻撃では攻撃 SYN パケットの送信元 IP アドレスがランダムに偽装されおり，そのような場合では N_T は 0 に近い値を取り，送信元 IP アドレスの重複があったり前述の図 3 のような高度な攻撃に対しても N_T の値を小さく抑えることができる．なお，TCP Intercept のみで防御を行った場合は $N_T = P$ となり，P 個すべての攻撃 SYN パケットに代理応答を行わなくてはならない．

これにより，提案手法は多くの攻撃 SYN パケットに対しては SYN Drop のアイデアで防御を行い，代理応答のためのパケット生成やその送信の処理を省くことができるため，その分の負荷を軽減できることが期待できる．

4.2.2　認証の強度

3.2.3 項で示した通り，SYN Drop は TCP Intercept の代理応答と比較して認証が強固でなく，攻撃者が同一の送信元 IP アドレスの SYN パケットを二重で送信することで再送を偽装し防御をバイパスされてしまう可能性がある．それに対して提案手法は，再送を偽装した SYN パケットに対して TCP Intercept のアイデアで代理応答を行うため，攻撃パケットをサーバーに到達させずにドロップすることができる（図 5）．

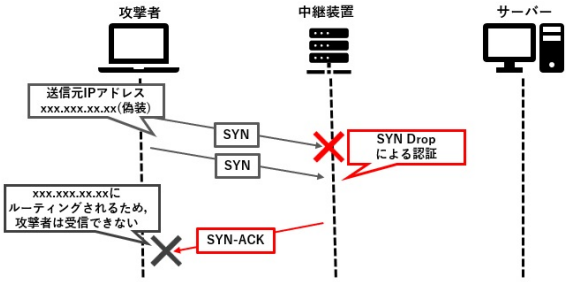

図 5　同一 SYN パケットの二重送信に対する提案手法の防御

4.3　提案手法の問題点

提案手法は，負荷と認証の観点で TCP Intercept と SYN Drop のそれぞれの利点を活かせることが期待できる一方，正規のクライアントが新規に接続する際の遅延が増大することが想定される．正規のクライアントの初回接続時は，SYN Drop と TCP Intercept のセッション管理を順番に行い認証を受けるため，両手法の遅延を合算した程度の時間が総遅延時間となると考えられる．なお二回目以降の接続時は，すでに認証を受けているため特別な遅延は発生しない．

5.　実験

本章では，提案手法の有効性を検証するために行った三つの比較実験とその結果について述べる．

5.1　実験 1 の概要

4.2.1 項で，提案手法が TCP Intercept と SYN Drop のハイブリッド型の防御を行うことで、TCP Intercept 単体で用いるよりも軽量な防御を行える可能性があることについて考察した。一方で，SYN Drop が低負荷であることは関連研究 [8] で示唆されているものの明確な検証は行われておらず，TCP Intercept と比較してどの程度差があるのかも不明瞭である．

そこで実験 1 では，SYN Drop と TCP Intercept をそれぞれ中継機器に実装し，SYN Flood 攻撃を行うことで，実際に TCP Intercept と SYN Drop でどの程度処理負荷に差があるのかを確かめる．

5.2　実験 2 の概要

実験 2 では，4.2.2 項で考察した SYN Drop をバイパスし得る攻撃シナリオについて，中継機器に提案手法と SYN Drop をそれぞれ実装し，攻撃シナリオのシミュレーションを行うことで，実際に攻撃シナリオが SYN Drop に対して有効であることと，それを提案手法では防御できることを確認する．

5.3　実験 3 の概要

実験 3 では，4.2.3 項で考察した提案手法の問題点である

初回接続時の遅延について，各手法での遅延を計測し，提案手法の遅延が既存手法と比べてどの程度大きいかを検証する．

5.4 実験環境

本実験では，データリンク層で動作するブリッジベースとした中継装置を用いて実験を行った（図 5）．通常，ブリッジは複数のネットワークインターフェース間で L2 パケットを転送する．本実験では Linux PC 上で動作するブリッジを設計し，通常の動作に加えて，パケットを解析し提案手法と既存手法の防御を行うプログラムをそれぞれ実装した．中継装置としてブリッジを選択した理由としては，ルーターやプロキシと比較して動作が単純であるため，アルゴリズムの負荷の比較検証に適しており実装も容易であることが挙げられる．

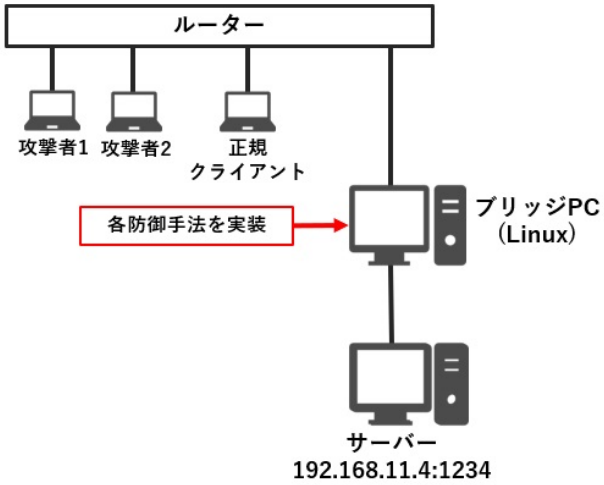

図 6 実験環境の概略図

5.5 実験 1: 中継装置の負荷の計測

攻撃者がサーバーに SYN Flood 攻撃を実施し，そのとき中継装置にかかる CPU 負荷を計測する．サーバーに対して送信元 IP アドレスをランダムに偽装した SYN パケットを大量に送信し，パケットがサーバー到達前に中継装置であるブリッジを中継したときに，それぞれの防御手法に基づいて処理する．防御手法は TCP Intercept と SYN Drop をそれぞれ実験し，負荷の比較を行う．

5.5.1 実験方法

攻撃トラフィックの生成には Hping3 を用い，一定の送信レートで 1 分間攻撃を行ったときの中継装置の平均 CPU 使用率とパケットロス率を測定する．この測定をいくつかの送信レートで行うことで，送信レートを増大させていったときの平均 CPU 使用率とパケットロス率の推移を調べる．

5.5.2 実験結果

実験結果，平均 CPU 使用率図 7 のように推移した．両手法ともに攻撃レートが高くなるにつれ CPU 使用率も高くなり，TCP Intercept よりも SYN Drop のほうが全体的に低く推移していることが読み取れる．また，両手法ともに攻撃レートが 74000pps 程度のときに平均 CPU 使用率が大きく下がっているが，これは後述するパケットロスの影響だと考えられる．

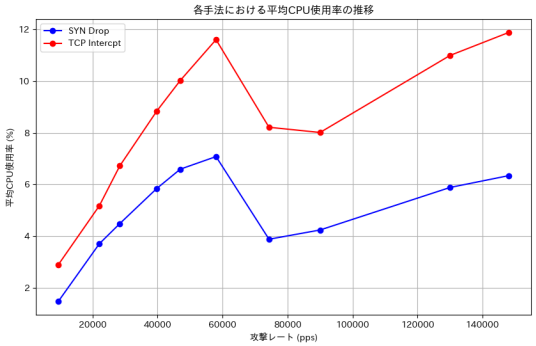

図 7 各手法において攻撃レートを変化させたときの中継装置の平均 CPU 使用率の推移

パケットロス率の推移は図 8 のようになった．両手法ともに攻撃レートが 74000pps 程度のところからパケットロスが発生しはじめ，その後の推移にも大きな差は見られなかった．

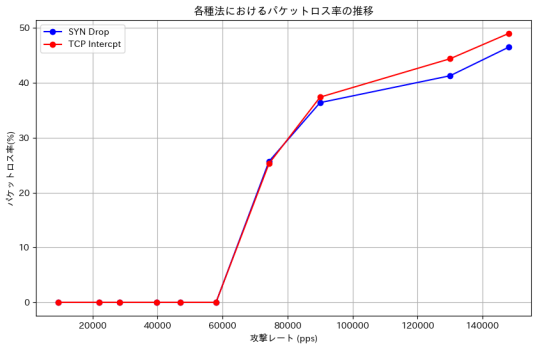

図 8 各手法において攻撃レートを変化させたときの中継装置のパケットロス率の推移

5.6 実験 2: 高度な攻撃への対応

3.2.3 項の図 3 のような SYN Drop の認証をバイパスし得る攻撃を実施し，そのときサーバーにどの程度攻撃パケットが到達するかを検証する．防御手法は SYN Drop と提案手法をそれぞれ実装して，提案手法が SYN Drop では防御しきれない高度な攻撃に対しても対応できるかを確かめる．

5.6.1 実験方法

scapy を用いて送信元 IP アドレスを偽装した攻撃 SYN パケットを生成し，一つの送信元 IP アドレスにつき二回送信したときの，サーバーの half open ソケット数を netstat コマンドで測定する．攻撃は 1 分間行い，時間推移を記録する．

5.6.2 実験結果

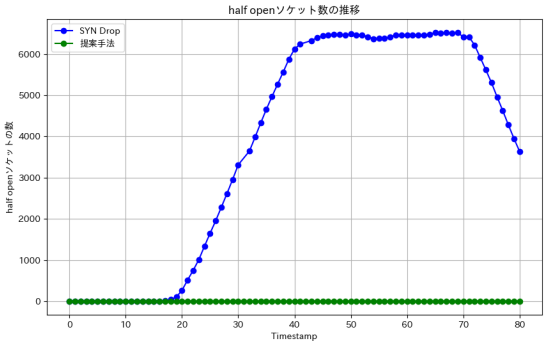

図 9 各手法におけるサーバーの half open ソケット数の時間推移

実験結果は図 9 のようになった．SYN Drop による防御では．認証がバイパスされてサーバーに攻撃パケットが到達し，結果 syn backlog が飽和していることがわかる．一方で提案手法では，攻撃パケットはサーバーに一つも到達させずに防御できていた．

なお実験 2 では scapy を用いて高度な攻撃を試験的に実装・シミュレートしたため，実験 1 で Hping3 を用いたときよりも攻撃レートは低くなった．

5.7 実験 3: 初回接続時の遅延の計測

正規のクライアントがサーバーに対して新規に接続を試みた際の遅延を測定する．Simple Bridge（防御を行わない単純なブリッジ）,SYN Drop,TCP Intercept, 提案手法の四種を実装した場合でそれぞれ遅延を測定し，比較を行う．

5.7.1 実験方法

curl コマンドの time_starttransfer オプションを用いて HTTP リクエストを送信し，サーバーからのレスポンスとして最初のバイトを受信するまでにかかった時間を測定する．

5.7.2 実験結果

実験結果は図 10 のようになった．初回接続時の遅延は提案手法,SYN Drop,TCP Intercept,Simple Bridge の順で長く，提案手法では SYN Drop と TCP Intercept のそれぞれの遅延時間を合計した程度の遅延が発生していることを確認した．なお，二回目以降の接続では，いずれの手法も Simple Bridge と同等の遅延であった．

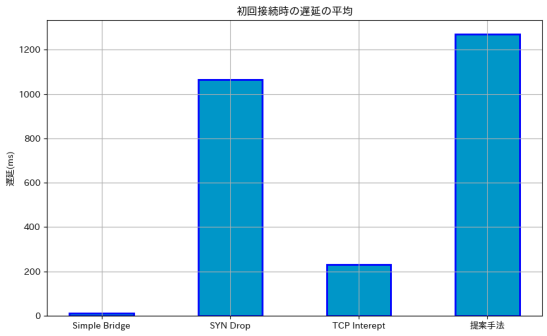

図 10 Enter Caption

6. 考察

本章では，第五章で行った実験の結果の考察について述べる．

6.1 実験 1 の考察

実験の結果，SYN Drop は TCP Intercept よりも低負荷で防御を行えていることが確認できた．したがって提案手法においても、送信元 IP アドレスをランダムに偽装した攻撃 SYN パケットに対し SYN Drop のアイデアで防御を行うことで，高負荷な代理応答処理を省き負荷の増大を抑えることが期待できる．一方でこの処理負荷の差がどの程度有意であるのか，さらにレート上げたときにどのようにスケールするのかについては後述のパケットロスの件も併せて今後の課題として検討したい．

パケットロスが発生するレートに関しては，有意な差が見られなかった．ここには防御プログラムの負荷だけではなく NIC やネットワーク機器の性能も影響している可能性があるため，それらも踏まえたうえで実験環境を再考する必要がある．

6.2 実験 2 の考察

提案手法は，高度な攻撃に対しても SYN Drop と TCP Intercept それぞれのアイデアで二段階の認証を行うことにより，SYN Drop では防御できない攻撃に対しても対応できていることがわかった．代理応答による認証をバイパスするためには，SYN-ACK パケットのシーケンス番号を予測し適切な ACK パケットを偽装する必要があるが，通常 SYN-ACK パケットのシーケンス番号はランダムに設定されるため予測は困難であるため，強固な認証であると考えられる．

6.3 実験 3 の考察

提案手法の課題として挙げられていた遅延について，実際に既存手法よりも大きくなってしまっていることを確認した．大きな遅延が発生するのは初回接続時のみであり二

度目以降の接続では遅延はほぼ発生しないが，サービスによっては遅延の増大は致命的ではある．そのため，攻撃発生時にのみ限定的に防御手法を適用する必要があり，適切な攻撃検知アルゴリズムの検討が今後の課題として挙げられる．

また，今回の実験において SYN Drop による遅延は 1000ms 程度であったが，これは OS に設定されている再送までの時間に依存するため，クライアントの環境によって変化することに留意する必要がある．

6.4 実験全体の考察

本実験では，4 章で議論した処理負荷, 認証の強度, 遅延の 3 つの観点から，実際に各手法をそれぞれ実装して検証を行った．その結果，4.2.1 と 4.2.2 項のとおり，提案手法は SYN Drop の処理の軽量さと TCP Intercept の認証の強固さを両立した防御を行える見込みを得ることができた．一方で 4.2.3 項のとおり，既存手法と比べて初回接続時の遅延が発生することも確認されたため，遅延の影響を最小限に抑える手法について検討を進める必要がある．

7. まとめ

DoS・DDoS 攻撃は，デジタル化が急速に進展する昨今において依然として大きな脅威となっている．その中でも SYN Flood 攻撃は，攻撃コストが低く汎用性も高い一方で，攻撃トラフィックと通常トラフィックの区別は容易ではなく，有効な防御・緩和手法が望まれる．先行研究では，サーバーとクライアント間の中継機器で動作するネットワークベースの防御手法の有効性の検証が進められてきたが，攻撃パケットのフィルタの精度が十分でなかったり，中継装置に大きな負荷がかかったりするなどの問題がある．

本研究では，ネットワークベースの既存手法である TCP Intercept と SYN Drop を組み合わせて用いることで，低負荷かつ強固な防御を行う手法を検討した．提案手法のアルゴリズムについて，負荷，認証の強度，遅延の観点から分析を行い，既存手法と比較検証を行うことでその有効性について考察した．

実験結果から．提案手法は SYN Drop と同程度に低負荷でありながら，TCP Intercept と同等の強固な防御が可能である見込みを得た．そのため，検知手法では，防御の堅牢さを保ちつつ，処理負荷を改善することができる可能性があると考えられる．

一方で，正規のクライアントが初めてサーバーに接続したときの遅延は従来手法よりも大きくなっていることが今後の課題であり，攻撃を適切に検知しそのときのみ局所的に動作するアルゴリズムを検討する必要がある．それによって，遅延が発生する機会を減らし，遅延によるインパクトを最小限に抑えることができると考えられる．

また，4.2.1 項で行った処理負荷の定式化についても，R,W,G,O と置いたそれぞれの処理負荷（命令数）が実際どの程度のものであるのか，処理負荷の尺度として命令数が妥当であるのか，といったことについてもさらに検討を進めたい．

参考文献

[1] Kaspersky,"DDoS report: Q3 2022", Nov 2022.
[2] S. S. Kolahi, A. A. Alghalbi, A. F. Alotaibi, S. S. Ahmed and D. Lad, "Performance comparison of defense mechanisms against TCP SYN flood DDoS attack," 2014 6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), St. Petersburg, Russia, 2014, pp. 143-147.
[3] S. T. Zargar, J. Joshi and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," in IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2046-2069, Fourth Quarter 2013.
[4] S. T. Zargar and J. B. D. Joshi, "A collaborative approach to facilitate intrusion detection and response against DDoS attacks.," 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2010), Chicago, IL, USA, 2010, pp. 1-8.
[5] J. Postel, "Transmission Control Protocol," RFC 793, IETF, Sept 1981.
[6] J. Lemon, "Resisting SYN flooding DoS attacks with a SYN cache," Proceedings of USENIX BSDCon'2002, pp.89–98, February 2002.
[7] A. Zuquete, "Improving the functionality of SYN cookies," Proceedings of 6th IFIP Communications and Multimedia Security Conference, pp.57–77, September 2002.
[8] P. Goldschmidt and J. Kučera, "Defense Against SYN Flood DoS Attacks Using Network-based Mitigation Techniques," 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), Bordeaux, France, 2021, pp. 772-777.