C-10

多段 DRIP を用いた DoS 攻撃に対する防御手法の提案

中川　慶祐 †　　川橋　裕‡

Keisuke Nakagawa　Yutaka Kawahashi

1. はじめに

近年，インターネットの普及や高速化が進み，多くの企業や機関ではネットワークを用いてサーバを外部に公開している．一方，インターネットを介したサービス提供の阻止や，金銭の要求を目的とする DoS 攻撃(Denial of Service attack)[1]の事案が増加の一途をたどっている．防御を行う際の問題点は，正規の通信との区別がつきにくい点である．このため，既存防御手法である FireWall では攻撃を対処しにくい．既存研究では DoS 攻撃に対し，ソースアドレスルーティングを実装したルータである DRIP を用いた防御システムの有用性が示された．

2. 既存研究

B-DRIP とは，秒間パケット数と保護対象サーバの CPU 使用率によって DoS 攻撃を検知する．保護するサーバ毎に，閾値を設定することが可能である．DoS 攻撃に対する防御手法には，ソースアドレスルーティングを用いて攻撃者からのパケットを代理応答サーバにパケットを転送することで防御をおこなう．

既存研究の B-DRIP では 3 つの問題点がある．まず 1 つ目は，攻撃検知と攻撃対処を 1 つのサーバでおこなうため，負荷が集中する点である．また，故障した際には攻撃の検知と対処のどちらもおこなえなくなる．2 つ目は，攻撃者が複数存在する際，同時に対処できない点である．既存研究では，攻撃を検知した際，単位時間内にアクセスが一番多かった IP アドレスを攻撃者と判別し代理応答サーバにパケットを転送する．そのため，複数の攻撃元の対処に時間を要する．3 つ目は，攻撃検知に閾値を使用している点である．CPU の性能や時間帯により使用率が変化するため，一時的にアクセスが集中した際には攻撃を受けていると判別してしまう．そのため，特定の状況下では誤検知が多く発生することになる．

3. 研究目的

本研究では 2 章で述べた問題点を解決するために，B-DRIP を攻撃検知部と攻撃対処部の 2 つに多段化することにより，負荷を分散することを 1 つ目の目的とする．また攻撃検知にはシグネチャ型の IDS を導入し，誤検知や攻撃の見逃しの低減を 2 つ目の目的とする．さらに，攻撃者の対処には管理者が事前に Web サーバにアクセスを許可するリストを作成する．攻撃を検知している期間，そのリストを参照し Web サーバに対するアクセスをコントロールすることを，3 つ目の目的とする．

4.　提案システム

本研究では，B-DRIP を攻撃検知部と攻撃対処部にわけ，負荷を分散させた．攻撃検知部では，攻撃を検知するためにシグネチャ型の IDS(Intrusion Detection System)である Snort[3]を導入した．Snort とは，ネットワーク型の IDS である．ネットワーク上を流れる IP パケットをキャプチャし，攻撃パケットを定義したシグネチャと呼ばれるルールと比較することで，攻撃を検知する．攻撃を検知した際は，攻撃対処部に IP

†和歌山大学大学院, Graduate School of Systems Engineering, Wakayama University

パケットを転送する．攻撃対処部では，管理者が事前に Web サーバにアクセスを許可する IP アドレスリストを作成しておく．攻撃検知部から転送されて来た IP パケットを受け取ると，IP アドレスリストを参照する．事前に登録されている場合，Web サーバに IP パケットを転送する．それ以外の場合，/dev/null に転送し IP パケットを破棄する．

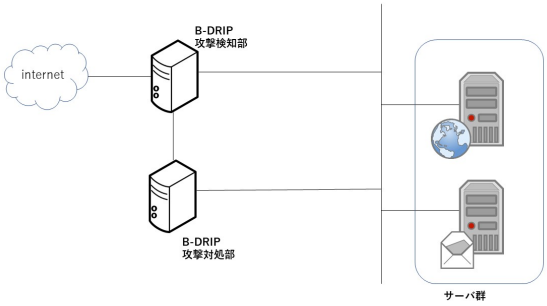

図 1　提案システム

5.　評価実験

本提案システムの有用性を示すために評価実験を実施した．評価実験は負荷分散実験，攻撃検知実験，攻撃対処実験の 3 種類である．

5.1 負荷分散実験

本実験では，攻撃検知部と攻撃対処部を 1 つのサーバにまとめた場合と，提案システムのように 2 つに分けた際のサーバの CPU 使用率を確認した．実験結果を図 2 に示す．

5.2 攻撃対処実験

本実験では，攻撃検知部の Snort で攻撃が検知可能であるかを確認した．今回，SSH に対するブルートフォース攻撃と Web サーバに対する SYN Flood 攻撃を実施し，検知結果を図 3 と図 4 に示す．

5.3 攻撃対処実験

本実験では，複数端末からの攻撃の際でも，同時に攻撃を対処することが可能であるかを確認した．実験結果を図 5 に示す．

6.　評価

既存研究の B-DRIP では，攻撃の検知と対処を一つのサーバでおこなっていた．それに対し本システムでは，攻撃の検知と対処を別々のサーバでおこなう．実験の結果より負荷が分散されていることが確認できる．また，既存研究では保護対象の Web サーバの CPU 消費率に閾値を設定し攻撃を検知していた．それにより，閾値を下回る攻撃に対して攻撃を検知することが不可能であった．しかし本システムでは，既存研究で検知できなかった攻撃を IDS で検知することにより，攻撃の見逃しを低減することが可能となった．さらに，様々なプロトコルに対応可能であり，Web サーバだけでなく DNS サーバ，メールサーバなど様々なサーバに対して保護することが可能となった．また，攻撃対処は複数からの攻撃の場合でも，管理者が事前に作成した Web サーバに対するアクセスを許可する IP アドレスのリストを参照し，コントロールすることにより，同時に複数の攻撃者の対処が可能となった．

7.　終わりに

本提案システムでは，IDS である Snort を導入し攻撃の検知を実施している．しかし，管理者が事前に設定するシグネチャに記載されていない攻撃に対しては，無防備である．新種の攻撃にも対応するべく，シグネチャ型ではなく，正常を定義するアノマリ型の IDS の導入を目指す．また，攻撃対処部で参照する，Web サーバにアクセスを許可する IP アドレスリストに記載されている IP アドレスからの攻撃に対処するべく，攻撃者を特定するシステムの導入を目指す．

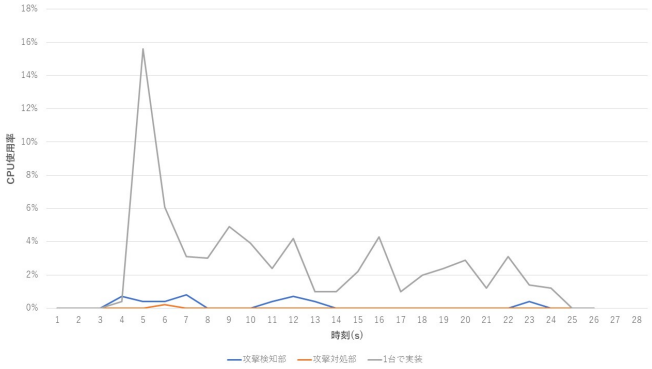

図 2 負荷分散実験結果

図 3SSH へのブルートフォース攻撃の検知結果

図 4 SYN Flood 攻撃の検知結果

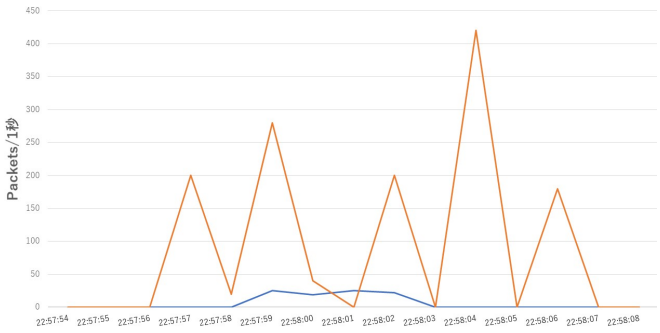

図 5 攻撃対処実験結果

参考文献

[1]”サービス妨害攻撃の対策調査”

IPA 独立行政法人 情報処理推進機構

https://www.ipa.go.jp/files/000014123.pdf

[2]”サーバリソース状況に基づいた DoS 攻撃対処システムの構築”

平 和規

2012 年度 和歌山大学 卒業論文

[3]Snort オフシャルサイト

https://www.snort.org/