Vol.2015-DPS-162 No.19
Vol.2015-CSEC-68 No.19
2015/3/5

経路変更を用いた分散フィルタリングによる DNS amp 攻撃への対策手法の提案

桂井友輝[†1]　中村嘉隆[†2]　高橋修[†2]

近年，DDoS 攻撃の被害が全世界で急増し，ネットワークサービス提供者にとって非常に深刻な問題となっている．中でも，対策が施されていないキャッシュ DNS サーバ，家庭用ルータを悪用することで対象へ容易に被害を与える DNS amp 攻撃に注目が集まっている．DNS amp 攻撃への対策として，ファイアウォールやサーバの設定によるフィルタリングなどが挙げられる．しかしこれらの手法では，回線の飽和に起因するネットワークへの被害を抑えることができず，またフィルタリングを行う端末への負荷による悪影響が考慮されない．本稿では，インターネットバックボーンから被害を受ける各サービスへのネットワーク中継点にスイッチを設置し，攻撃パケットを複数の端末へ振り分け分散フィルタリングを実行させることで，ネットワークへの被害縮小，フィルタリングを行う端末の負荷削減を目的とした手法を提案する．

キーワード： DDoS 攻撃，DNS amp 攻撃．カプセル化，iptables，UDP，フィルタリング

A countermeasure method against DNS amplification attacks by dispersion filtering using traffic route change

YUKI　KATSURAI[†1]
YOSHITAKA　NAKAMURA[†2]　OSAMU　TAKAHASHI[†2]

1. はじめに

近年，情報化社会の発展に伴い，インターネットを利用するサービスは身近なものとなった．しかし同時に，サイバー攻撃による被害も急増している．ネットワークを構成する機器に対して攻撃し，サービスの提供を阻害する攻撃である DoS 攻撃(Denial of Service attacks)，またボットネットを利用し．踏み台と呼ばれる多数のコンピュータによって DoS 攻撃を仕掛ける DDoS 攻撃(Distributed Denial of Service attacks)などが存在しており，非常に大きな問題となっている．この DDoS 攻撃の中でも，代表的な攻撃の一種として長年利用され続けているのが，DNS amp 攻撃(DNS amplification attacks)である．

DNS amp 攻撃とは，DNS サーバを利用した増幅攻撃を表す．DNS サーバは送信元からの問い合わせ（名前解決要求）に対し反射的に大きなサイズの応答を返すリフレクターとしての特性と，増幅器としての特性を持っており，DNS amp 攻撃にはこれらの特性が悪用される．RFC 5358/BCP 140 においては，正式には Reflector Attacks（DNS リフレクター攻撃）と定義されているが[1]，本稿では一般に称される DNS amp 攻撃で統一する．図 1 に DNS amp 攻撃の概要を示す．

攻撃者から DNS サーバに対し，送信元 IP アドレスが偽造された名前解決要求が送信される．これを受けた DNS サーバが，偽装された IP アドレス，即ち被害者に向け応答を返す．これによってネットワークの輻輳，被害者の処理能力への過負荷を招く攻撃が DNS amp 攻撃である．この攻撃の危険性に関しては 2001 年段階から指摘されていた[2].

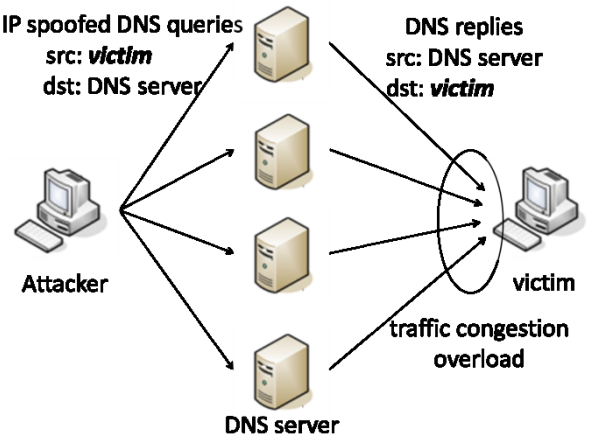


図 1: DNS amp 攻撃の概要

DNS サーバには，権威 DNS サーバとキャッシュ DNS サーバの 2 種類が存在する．権威 DNS サーバとは，自身が管理するドメイン名空間の一部を他の複数の DNS サーバと共有し，ツリー構造を形成することでデータの分散的な管理を行う DNS サーバである．キャッシュ DNS サーバとは，リゾルバとも呼ばれ，クライアントから名前解決要求を受けた際に権威 DNS サーバに対し問い合わせを行い，結果をクライアントに返す DNS サーバである．このとき，本来であれば必要のない名前解決機能が有効にされている権威 DNS サーバ，また外部から送信された名前解決要求の処理

†1 公立はこだて未来大学大学院　システム情報科学研究科
Graduate School of Systems Information Science, Future University Hakodate
†2 公立はこだて未来大学　システム情報科学部
School of Systems Information Science, Future University Hakodate

を行ってしまうキャッシュ DNS サーバを併せてオープンリゾルバと呼ぶ. 家庭用ルータにもキャッシュ DNS サーバとしての機能が備わっており，オープンリゾルバとして攻撃に利用される事例も発生している.

2. 関連研究

DNS amp 攻撃への対策としては, DNS が増幅器として利用されることを防ぐもの，また実際に攻撃が行われた場合に被害者側が自衛のために行うものが存在する．以下，各対策について述べる.

2.1 DNS が増幅器として利用されることへの対策

DNS サーバが他者への攻撃に利用されないようにするための対策は，予防としての役割を果たすものである．この種の対策手法として, キャッシュ DNS サーバ, 権威 DNS サーバをそれぞれ DNS amp 攻撃に利用されないための手法が挙げられる．各手法について以下に述べる.

2.1.1 キャッシュ DNS サーバにおける対策

キャッシュ DNS サーバに施す DNS amp 攻撃への対策としては，アクセスコントロールの実施，ルータによるパケットフィルタリングが存在する.

アクセスコントロールに関しては，DNS 問い合わせについて，IP アドレスベースでキャッシュ DNS サーバのサービス対象とするクライアントからのアクセスのみを許可する．図 2 にアクセスコントロールの概略図を示す.

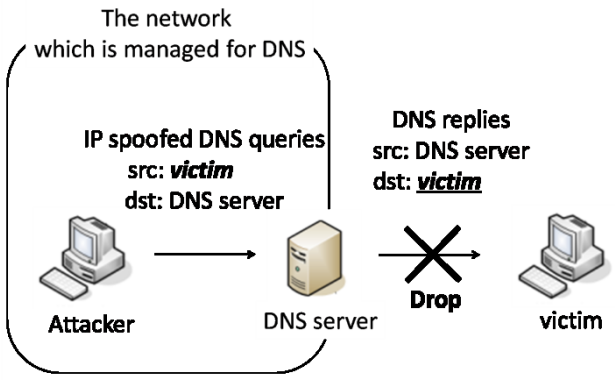


図 2: アクセスコントロールによる対策

図 2 では，DNS サーバが管理するネットワーク外に存在する被害者を DNS amp 攻撃の対象に設定した場合を表している．この際，DNS サーバ側の設定により，キャッシュ DNS サーバからサービス対象外の被害者に送信される応答がドロップ (破棄) されることになり, 外部への DNS amp 攻撃の踏み台として利用されるリスクが軽減される．この対策に関しては, RFC 5358/BCP 140 内で述べられている[1].

パケットのフィルタリングは, 送信元 IP アドレスが詐称されたパケットの送受信を防ぐ設定をルータなどのネットワーク機器に施すことである．詐称パケットの通過を阻止することによって, 対象の DNS サーバに詐称パケットが到達せず, 結果的に攻撃を防ぐこととなる. これに関しては, Source Address Validation（送信元検証）という名称で RFC 2827/BCP 38, また RFC 3704/BCP 84 に記されており[3][4], DNS amp 攻撃だけでなく様々な攻撃への対策として用いられている.

2.1.2 権威 DNS サーバにおける対策

権威 DNS サーバにおいては, 名前解決要求の送信元はキャッシュ DNS サーバである. またインターネット全体にサービスを提供するため，キャッシュ DNS サーバと同様の IP アドレスによるアクセスコントロールでは不都合が生じる．ボットネットなどを利用し広範囲から問い合わせを受けた場合などは，アクセスコントロールでは対応することができない. また, 権威 DNS サーバを利用した DNS amp 攻撃では, DNS の応答パケットのサイズが大きくなる傾向があり，更なる対策が求められる．この事実を受け，Paul Vixie らによって DNS RRL (DNS Response Rate Limiting)が提案された[5]．これは DNS amp 攻撃の最中，権威 DNS サーバが短時間に同じ宛先に対し高頻度で同じ応答を返すことを利用した対策である．応答頻度を監視し，一定の割合を超えた場合は応答の制限，破棄を行う．またこの際，同じ応答と判断するポイントを柔軟に変更することで，多様な攻撃に対応することが可能となる．図 3 に，DNS RRL による対策の一例の図を示す.

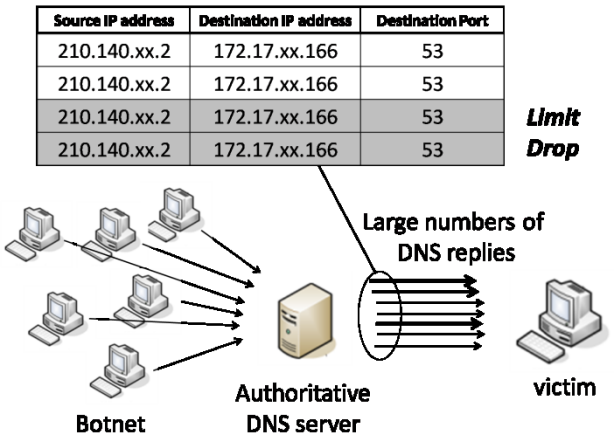


図 3: DNS RRL による応答制限

DNS RRL を適用する上での問題点としては, 誤検出の発生が挙げられる．統計的に攻撃の判断を行うため，本来検出するべきではないパケットを攻撃パケットとみなしてしまう事象が存在する．この誤検出の抑制のため，応答の破棄を行う際，キャッシュ DNS サーバに対し TCP による再送の要求を行い, 正常な名前解決を可能としている. また, Rozekrans らによって，DNS RRL の実証実験の結果が示されている[6]. この文献では DNS dampening と呼ばれるクラ

Vol.2015-DPS-162 No.19
Vol.2015-CSEC-68 No.19
2015/3/5

イアントごとに評価値を与える手法と併用しており，現在存在する攻撃への有用性を示すとともに，今後発展する攻撃への対応には送信元検証などとの併用が求められると述べている．

2.2 被害者が自衛のために行う対策

DNS amp 攻撃への理想的な対策は，世界中全てのネットワーク機器へ一斉に送信元検証を適用することであるが，それは現実的ではない. 次善の策として存在するのが, DNS サーバへのアクセスコントロール, DNS RRL の適用である. しかし, DNS RRL についてはまだ研究が進められている状況であるとともに，それらの対策はネットワーク，DNS サーバの管理者が個々で行うべきものであり，対策が施されていない機器，また DNS サーバについては，依然踏み台として攻撃に悪用されてしまう．そのため，被害者側には自衛手段として DNS amp 攻撃への対策が求められる. その際に用いられるのが，被害者側のネットワークで行うフィルタリングである．

被害者側のネットワークにおいて，攻撃の検知とファイアウォールにおけるフィルタリングを行う手法が Ye らによって提案されている[7]．この手法では，バックボーンであるインターネットから被害者の提供するサービスへと至るネットワークの道中において，パケットのミラーリングを行い DDAA(Detecting DNS Amplification Attack)と名付けられたシステムへと送信するスイッチを設置する．このシステムはスイッチから受け取ったパケットの情報を記録し，その後，記録した情報から攻撃と思わしきパケットをファイアウォールでブロックする. 図 4 に DDAA を含むフィルタリング手法を示す.

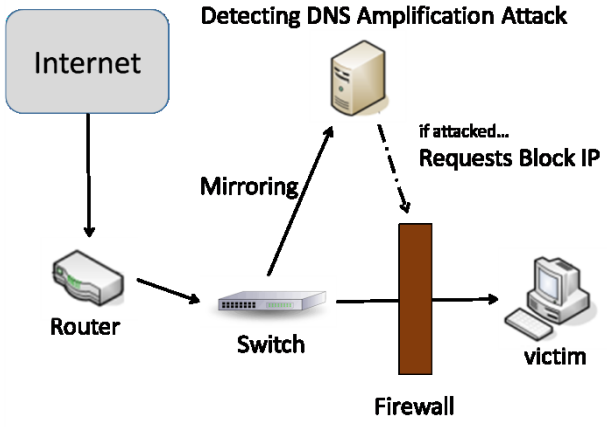


図 4: DDAA によるフィルタリング手法

この手法では，DDAA 内のデータベースに通過するパケットの IP アドレス, 宛先ポートなどの情報を保持することになる．そのため時間が経過するごとにシステムのパフォーマンスが低下する．そのため，データベースに保存したパケットの情報が 10000 を超えた場合，3 秒以上保持した情報を全て削除するように設定してある．この手法の利点は，DDAA のパラメータ設定によってフィルタリングの情報を動的に更新，保存できる点である．検知とブロックを同一端末で管理することにより, いくつかの DNS 応答パケットが被害者のもとへ到達した後に，続いて送信される DNS 応答パケットを直接的にファイアウォールによってドロップすることができる．この手法の問題点としては，ネットワークの輻輳，機器の負担に関して考慮されていない点が挙げられる．ファイアウォールの性質上，ネットワークへの輻輳に対応することができず，また常時データベースにパケットを保存，照合処理を行うことで，ファイアウォールと DDAA に高負荷がかかりパフォーマンスに影響を及ぼす可能性が存在する．

Paola らによって機器に低負荷な手法が提案されている[8]．この手法では，Bloom Filter を用いることで，通過するパケットを機器がデータベース内から効率的に検索することができる．そのため，機器にかかる負担が軽減され，また正確なフィルタリングを行うことができる．しかしこちらの手法に関しても，ネットワークへの影響が考慮されておらず，フィルタリングを行う際の輻輳による被害が度外視されている．

3. 提案手法

3.1 研究課題

本研究では，ネットワーク全体における対策が施されていない DNS サーバが攻撃に利用された場合を仮定し, 被害者側の自衛手段としてのパケットフィルタリングを扱う．攻撃検知後，被害者側のサービスに攻撃パケットが到達することが無いよう，ネットワーク道中でのフィルタリングを行う．またその際，複数のルータによる分散フィルタリングを行うことで，フィルタリングを実行するルータ，またその前後それぞれのネットワークへの負担を軽減する．

3.2 システム構成

本提案手法のシステムについては，バックボーンとしてのインターネット，インターネット内で被害者に近いところに存在するスイッチ，フィルタリングを行う複数台のルータ，統合に用いるルータ，そして被害者のサーバといった内容で構成される．システムの概略図を図 5 に示す.

Vol.2015-DPS-162 No.19
Vol.2015-CSEC-68 No.19
2015/3/5

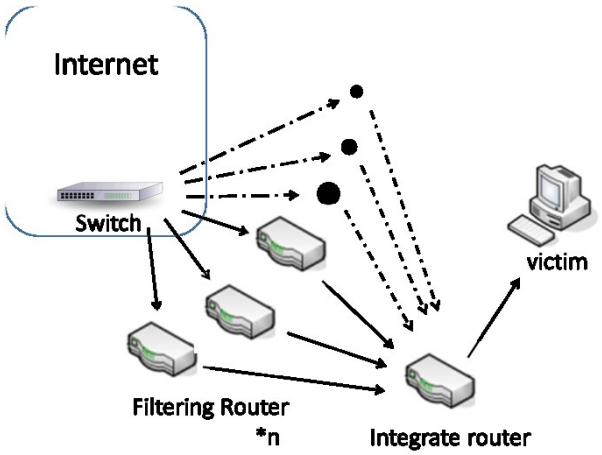


図 5: 提案手法概略図

インターネット内部から被害者のサーバへとパケットが送信される際，インターネットから各ネットワークへの接続点にスイッチを設置する．このスイッチからフィルタリングを行う任意台数のルータ(以下フィルタリングルータ)にパケットを分配し，フィルタリングを終えた後，統合用ルータによって正常な順序に戻してから被害者のサーバへと送信する．

3.3 処理概要

本提案手法に関しては，DNS amp 攻撃の検知に至るまで，検知後のパケットの分配，分散フィルタリング，フィルタリング後のパケットの統合という 4 段階に分けて処理が行われる．それぞれの内容に関して以下に記す．

3.3.1 DNS amp 攻撃の検知に至るまで

提案手法では，DNS amp 攻撃を検知するまでスイッチ，各ルータは特別な動作を行わず，既存の機器として同様の動作をする．また，複数台存在するルータに関しては，各自が構成しているネットワークの中でルータとしての役割を果たす．

3.3.2 攻撃検知後のパケット分配

DNS amp 攻撃を検知した際は，スイッチから各フィルタリングルータにパケットを分配する．分配する直前に，フィルタリングを行うルータに対し，フィルタリング開始命令と，どのルータが動作するかを通知する．例として，ルータ 1, ルータ 2, ルータ 3 の 3 台をフィルタリングルータとして設定する．このとき，ルータ 1 が平常時経路として用いられるルータであるとする．攻撃を検知した場合，規定量のパケットを塊としてカプセル化を施し，ルータ 1 に送信する．この時，カプセル化を施したパケットヘッドにはフラグメント情報を付加しておく．このフラグメント情報は，IP ヘッダにおけるフラグフィールド，フラグメントオフセットフィールドと似た意味を持ち，攻撃検知後から流したパケット全体における何番目の塊かという情報を示す．その後経路をルータ 2 に変更し，同様に規定量のパケットをカプセル化して，フラグメント情報を付加したものをルータ 2 に宛て送信する．ルータ 3 の場合も同様に行い，その後ルータ 1 に戻って以後同じ動作を繰り返す．また，フラグメントオフセットが上限に達した場合は，再度 0 から繰り返すように設定する．図 6 に，パケット分配の状況を示す．

パケット分配を停止する場合は，攻撃発生前に経路として用いていたルータ，例の場合ではルータ 1 に最後にパケットの塊を流した後，いくつかの塊を同じくルータ 1 に流し，その後パケットの分割を停止することで平常通りの通信を行う．これは，フラグメントオフセットを持たない塊が順序を乱し，結果的に通信に影響が出ることを防ぐためである．

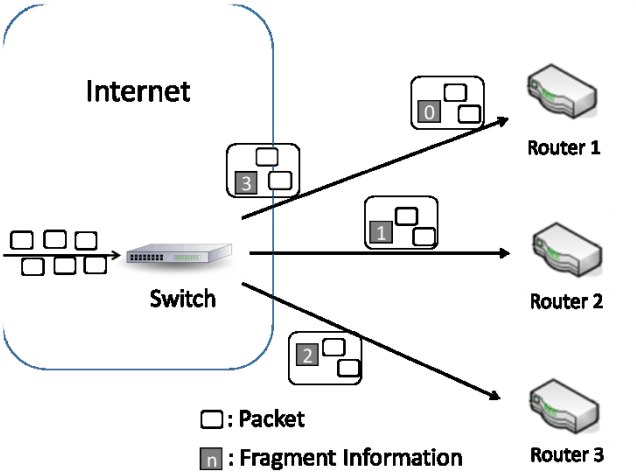


図 6: スイッチによるパケットの分配

3.3.3 分散フィルタリング

各ルータは，スイッチからフィルタリング開始の旨を通知されパケットの塊が流れてきた後，フィルタリング動作を開始する．第一に，DNS 応答パケットの特徴である，UDP53 番ポート宛であることがフィルタリングの条件として挙げられる．続いて，対象のパケットが UDP53 番ポート宛であった場合には，送信元 IP アドレスを自身の持つデータベースに登録する．その後同様の動作を繰り返し，規定時間内に一定量以上のパケットを送信してきた DNS サーバを踏み台に用いられたサーバとして認識し，その送信元 IP アドレスの情報を他のフィルタリングルータに対して送信，共有する．その後は対象の DNS サーバから送られてくる DNS 応答パケットを全てドロップする．図 7 にフィルタリングの様子を示す．

またフィルタリングを行う際，他のフィルタリングルータと共有した情報を除き，一定間隔でデータベースの初期化を行う．これは次々と登録されるパケットの情報に対して，検索効率をある程度の水準に保つための措置である．

Vol.2015-DPS-162 No.19
Vol.2015-CSEC-68 No.19
2015/3/5

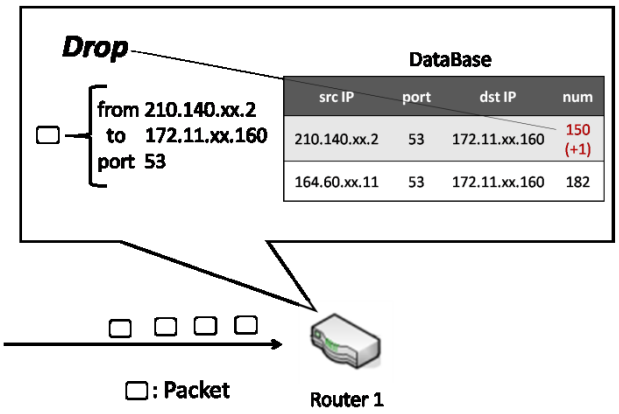


図 7: フィルタリングの様子

3.3.4 フィルタリング後のパケットの統合

フィルタリングルータは，塊ごとのフィルタリングを終えた後，統合用ルータへとパケットを送信する．統合用ルータでは，受け取ったパケットの塊を，スイッチが付加したフラグメントオフセットを参照することで正しい順序に並び替える．その後，番号が若い順に被害者のサーバ宛に送信する．

3.3.5 フィルタリング処理の関係性

以下に，提案手法のフィルタリング処理における他機器との関係性をまとめた図 8 を示す．

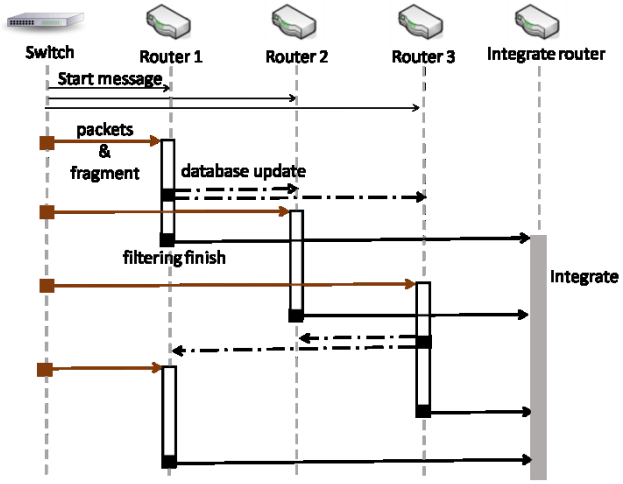


図 8: フィルタリング処理関係図

スイッチは動作開始後，フィルタリングルータに対して通知と，番号付けを行う．その後はパケットに一定量ごとのカプセル化を施し，フラグメントオフセットを記した後に宛先を Router1 から順に設定して送信する．

各フィルタリングルータは，フィルタリングを行う過程でデータベースに登録されていないパケットを新たに攻撃としてみなすことにした場合，その旨を他のフィルタリングルータに対し通知する．通知を受けたフィルタリングルータは，自身の持つデータベースを更新し，動作を継続する．

統合用ルータは，各フィルタリングルータから受信したパケットの順序を整理し，被害者サーバへと送信する．

3.4 提案手法の特徴

提案手法を用いることによって，インターネット内のスイッチから経路が分散され，被害者側のネットワークにおける輻輳の被害が軽減される．また，単一の端末でフィルタリングを行う場合と比較して，効率よくパケット情報の保存，参照を行うことができる．一方で，インターネット内のスイッチで輻輳が起こるレベルの攻撃に対しては，スイッチがボトルネックとなり劇的な効果は期待できないと予想される．また分散フィルタリング後のパケット統合に関しても，パケットロスなどが発生した場合など，特殊な対処が求められることが考えられる．

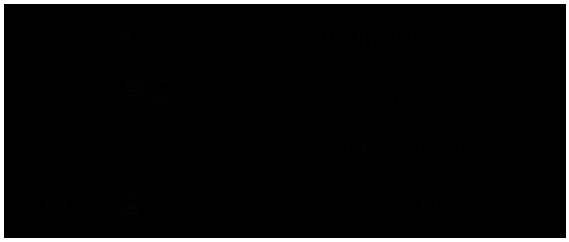
4. 実験

本稿における提案手法について，仮想環境による実装が完了した後に，評価実験を行う．以下，実験環境と実験内容，評価内容について述べる．

4.1 実験環境

実験環境として，仮想マシンをそれぞれ DNS サーバ，スイッチ，フィルタリングルータ，統合用ルータに見立てて設定し，攻撃シナリオを作成する．実験環境に関する表 1 を以下に示す．

表 1: 実験環境



4.2 実験内容

仮想環境内でコンピュータをスイッチ，ルータとして設定し，DNS サーバとして設定したマシンから通信を行う．攻撃開始から一定時間経過後，フィルタリングに関しては，データベースと iptables を用いることで，パケットのドロップ，通信の許可を管理する．

4.3 評価内容と考察

4.3.1 評価内容

以下の内容について実験結果の評価を行う．また，比較対象としては，ルータ 1 が単体でフィルタリングを行った場

合と，ルータ 1，ルータ 2，ルータ 3 による分散フィルタリングを行った場合を想定する．またルータ 2，ルータ 3 は他の通信も行っていることから，評価観点として，ルータの数を増やすことによるコスト面の比較は行わないものとする．

(1) スループット

単体でのフィルタリングを行った場合に関してはルータ 1 でのスループットを算出，分散フィルタリングを行った場合は 3 つのルータを総合したスループットを算出する．

(2) オーバーヘッド

単体でフィルタリングを行った場合はルータ 1 のオーバーヘッドを算出し，分散フィルタリングを行った場合では 3 つのルータそれぞれのオーバーヘッドを算出して平均値を取って比較する．

(3) パケットロス率

平常の通信も行われている環境下において，輻輳，誤検知などによるパケットロス率に関して，被害者サーバに到達したパケット数からパケットロス率を算出，比較する．

4.3.2 考察

実験を行うにあたり，想定される結果を考察する．

(1) スループット

システム全体としてのスループットは，攻撃規模が小さい場合には単体によるフィルタリングの方が高い．しかし攻撃の規模が大きくなれば，端末 1 台あたりの作業量が減少する文フィルタリング分散フィルタリングを行う提案手法に優位性が生じると想定される．

(2) オーバーヘッド

フィルタリングルータに関しては，単体でフィルタリングを行う場合と比較して単純に処理するべきパケット数が n 分の 1 となるため，明確に作業量が減少する．スイッチ側のカプセル化による負荷，またフィルタリングルータ間でのデータベースの共有に要する処理の影響を考慮する必要がある．

(3) パケットロス率

パケットロスが生じる原因として最も懸念されるのは，単体でフィルタリングを行う場合と同様，攻撃の誤検知である．スイッチによるカプセル化，統合用ルータでのパケットの統合に関しては，大きくパケットをロスすることは無いと想定される．

5. おわりに

本稿では，DNS amp 対策としての分散フィルタリング手法についての提案を行った．インターネットから各被害サーバの回線に移る際にフィルタリングを行う複数のルータへパケットを振り分けることで分散フィルタリングを実施し，単体でのフィルタリングの際に問題となる，フィルタリングを行う機器前後におけるネットワークへの被害を，単純な機器 1 台あたりのネットワーク負荷の面，また作業量によるパフォーマンス低下の面両方から緩和する．今後は実験を行い，提案手法における正当性，優位性を評価する．

参考文献

1) Damas, J., and Neves, F., “Preventing Use of Recursive Nameservers in Reflector Attacks,” RFC 5358, BCP 140 (2008).
2) Paxson, V., “An analysis of using reflectors for distributed denial-of-service attacks,” ACM SIGCOMM Computer Communication Review, Vol.31, No.3, pp.38-47 (2001).
3) Ferguson, P., and Senie, D., “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing,” RFC 2827, BCP 38 (2000).
4) Baker, F., and Savola, P., “Ingress Filtering for Multihomed Networks,” RFC 3704, BCP84 (2004).
5) Vixie, P., and Schryver, V., “DNS Response Rate Limiting (DNS RRL),” ISC-TN-2012-1-Draft1 (2012).
6) Rozekrans, T., and Koning, J., “Defending against DNS reflection amplification attacks,” University of Amsterdam System & Network Engineering RP1 (2013).
7) Ye, X., and Ye, Y., “A Practical Mechanism to Counteract DNS Amplification DDoS Attacks,” Journal of Computational Information Systems, Vol.9, No.1, pp.265-272 (2013).
8) Paola, S., and Lombardo, D., “Protecting against DNS Reflection Attacks with Bloom Filters,” Proceedings of the 8th international conference on Detection of intrusions and malware, and vulnerability assessment (DIMVA’11) , pp.1-16 (2011).