Vol.2016-DPS-166 No.26
Vol.2016-CSEC-72 No.26
2016/3/4

ネットワーク帯域への影響を考慮した DNS amp 攻撃に対する攻撃パケットフィルタリング手法の提案

桂井友輝[†1]　中村嘉隆[†2]　高橋修[†2]

概要：近年のネットワーク技術の発展に伴い，人々にとってネットワークは身近なものとなり，ネットワークを利用したサービスもまた広く展開されている．しかし同時にサイバー攻撃の被害も増加している．DNS amp 攻撃は DNS を悪用した DDoS 攻撃の一種であり，攻撃対象の処理能力やネットワーク回線を飽和させて，正常な利用を不可能なものとする．DNS amp 攻撃への対策としては主に DNS サーバ管理者による適切な設定変更，また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が挙げられる．しかし前者の手法は DNS サーバの管理者の知識，技術に依存する部分が大きく，家庭用ルータを利用した攻撃などには対応することが難しい．後者の手法では，回線の管理者，被害者が自ら能動的に対策できるという利点が存在するが，フィルタリングを行う端末への負荷，また攻撃に用いられる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ない．本研究では，フィルタリング手法による攻撃対策の改善を目的とし，フィルタリングを行う端末，ネットワーク回線への負荷を軽減するための分散フィルタリング手法を提案する．また攻撃パケットによりネットワーク回線に輻輳が発生している場合は，より上流に位置する，前後の帯域に余裕のある端末を基点としてフィルタリングを行う．ネットワークシミュレータ ns-3 上でネットワーク環境を作成し，提案手法を実装する．攻撃下における既存のフィルタリング手法との比較実験を行い，提案方式の有効性を評価する．

キーワード： DDoS 攻撃，DNS amp 攻撃，フィルタリング，帯域制御，経路制御

A Proposal of Attack Packet Filtering Method against DNS Amplification Attacks in Consideration of Effect on Networks Bandwidth

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

1. はじめに

近年，ネットワーク技術の発展に伴い，人々にとってネットワークは身近なものとなった．それに伴い，様々な分野でネットワークを利用したサービスが提供されている．しかしそれと同時に，分散型サービス拒否攻撃，DDoS 攻撃(Distributed Denial of Service attacks)をはじめとした，ネットワークを悪用するサイバー攻撃の被害も増加している．2015 年にロシアの Kaspersky 社が公開した調査結果[1]によると，従業員 50 人以上の企業の内およそ 20%の企業が過去に DoS 攻撃(Denial of Service attacks)，DDoS 攻撃の被害を受けていたと回答している．また同調査結果では，回答した内およそ 47%の企業が，DDoS 攻撃によってサービスが機能停止に追い込まれる事態に発展したこと，DDoS 攻撃の継続時間が数時間程度で終息するものから数週間にわたって継続したものまで様々であることが述べられている．

DNS amp 攻撃(DNS amplification attacks)は DNS (Domain Name System) [2][3]を悪用した DDoS 攻撃の一種である．対策が施されていないキャッシュ DNS サーバ，家庭用ルータを踏み台にすることで攻撃対象に大量のパケットを送信する．これにより，攻撃対象の処理能力やネットワーク回線を飽和させて，正常な利用を不可能なものとする．DNS amp 攻撃への対策としては主に DNS サーバ管理者による適切な設定変更，また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が挙げられる．しかし前者の手法は DNS サーバの管理者の対応に依存する部分が大きく，家庭用ルータを利用した攻撃などへの対処が難しい．後者の手法では，回線の管理者，被害者が自ら能動的に対策できるという利点が存在するが，フィルタリングを行う端末への負荷がボトルネックとなる可能性，また攻撃に用いられるネットワーク回線に大量のパケットが流入することにより輻輳が発生する可能性が存在する．

†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

2. DNS amp 攻撃

2.1 Domain Name System

Domain Name System とは，インターネット上で名前解決サービスを提供する分散型データベースシステムを指す．TCP/IP ネットワーク上においては，個々のコンピュータは IP アドレスと呼ばれる数値列で識別され，IP アドレスにはホスト名，ドメイン名と呼ばれる別名を付けることができる．DNS はこのホスト名，ドメイン名と IP アドレスの関

Vol.2016-DPS-166 No.26
Vol.2016-CSEC-72 No.26
2016/3/4

係の情報を管理し，外部からの問い合わせがあった際にそのドメイン名から元の IP アドレスやドメイン名に関連するメールサーバを引き出す動作を行う．これを名前解決といい，この動作に応答するコンピュータやソフトウェアを DNS サーバと呼ぶ．問い合わせの動作を行うコンピュータやソフトウェアをリゾルバと呼ぶ．図 1 に DNS サーバとリゾルバの動作の概略図を示す．

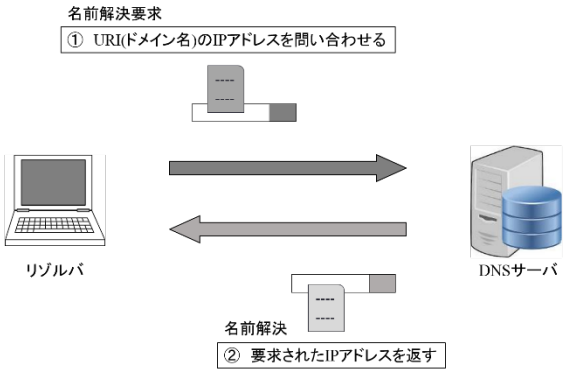

図 1: 名前解決

ドメイン名は階層構造をとっており，DNS サーバも同様に階層構造で管理される．上位にあたるドメインを保持する DNS サーバは下位のドメインを管理する DNS サーバの IP アドレスを把握している．

2.1.1 権威 DNS サーバ

権威 DNS サーバとは，DNS のデータベースを構成している DNS サーバの内，ドメイン名に関する完全な情報を保持したものの呼称である．主にドメイン名に関する問い合わせに対し回答を行うのはこの権威 DNS サーバである．しかし，インターネット上に多数存在する権威 DNS サーバは全てのドメイン名の情報を一括管理しているのではなく，それぞれ自身が管理するドメイン名空間に存在するドメイン名の情報のみを保持している．この権威 DNS サーバが管理するドメイン名空間の一部分を他のサーバと共有することで，データの分散的な管理が行われる．またこの情報は階層ごとに管理されており，起点となる空間を管理する権威 DNS サーバはルートサーバとも呼ばれる．

2.1.2 キャッシュ DNS サーバ

キャッシュ DNS サーバは，リゾルバの機能を有する DNS サーバのことである．クライアント端末のリゾルバから特定の名前解決要求を受けた際，階層が上位のルートサーバに対しドメイン名を問い合わせる．問い合わせを受けたルートサーバは自身が保持するいずれかのサーバへ問い合わせを行うよう回答し，キャッシュ DNS サーバは指定された権威 DNS へと問い合わせを行う．これらの動作を繰り返すことで，目的の URI の名前解決を行う．名前解決における権威 DNS サーバとキャッシュ DNS サーバの動作の一例を図 2 に示す．

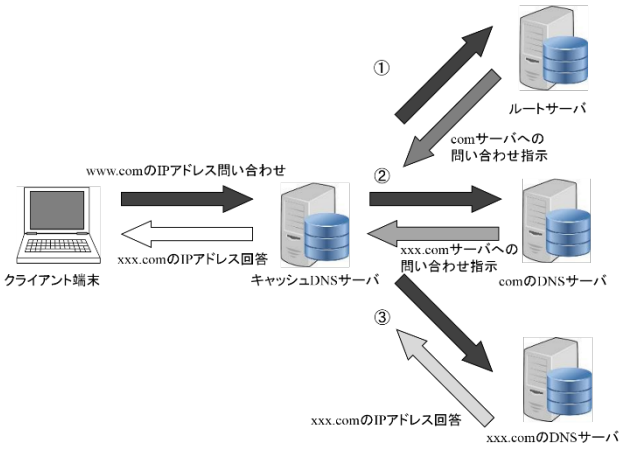

図 2: キャッシュ DNS サーバによる名前解決

2.1.3 オープンリゾルバ

オープンリゾルバとは，キャッシュ DNS サーバとして動作する DNS サーバの内，自身が所属するネットワーク外部に存在する不特定の IP アドレスからの問い合わせに対する応答を許可している DNS サーバのことである．基本的にキャッシュ DNS サーバ自体は自らドメインを管理することが無く，前項で述べた通り再帰的に権威 DNS サーバに問い合わせを行うことによって情報を取得する．本来は特定の組織やネットワーク空間などにおいて外部からの問い合わせを受け付けるべきではないとされている．しかし設定の不備などが原因となり，外部からの問い合わせに応答を行ってしまう．このオープンリゾルバは世界中に多数存在しており，キャッシュ DNS サーバとして運用されている DNS サーバだけでなく，一般的な企業や家庭でも用いられるブロードバンドルータなどのネットワーク機器が意図せずオープンリゾルバとして動作する事例も存在する．オープンリゾルバは様々な DDoS 攻撃の踏み台として悪用されることもあり，問題視されている．

2.2 攻撃概要

DNS amp 攻撃は，DDoS 攻撃の一種であり，代表的な攻撃手法として長年利用され続けている．前項で述べた通り，DNS サーバは送信元からの問い合わせ（名前解決要求）に対し反射的に応答を返すリフレクターとしての特性を持っている．加えて，問い合わせに対し一定長のデータを返すことから，増幅器としての特性も兼ね備えており，DNS amp 攻撃にはこれらの特性が悪用される．RFC 5358/BCP 140 [4] においては，正式には Reflector Attacks と定義されているが，本稿では一般に称される DNS amp 攻撃と統一する．DNS amp 攻撃においては，攻撃者から DNS サーバに対し名前解決要求が行われる際，パケットの送信元 IP アドレスに偽装が施されている．この送信元 IP アドレス偽装に関しては後述する．送信元 IP アドレスが偽装された名前解決要

求を受けた 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．大量の応答パケットによって被害者のコンピュータがこれらを捌ききれず通信不能に陥る，またはネットワーク回線の飽和による輻輳が発生するなどの事態を招く．また攻撃者はコンピュータウイルスに感染したコンピュータなどをボットコンピュータとして悪用する．DNS amp 攻撃の概要を図 3 に示す．

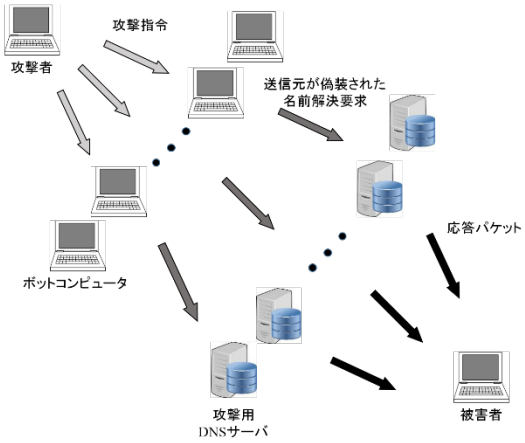

図 3: DNS amp 攻撃

2.2.1 送信元 IP アドレスの偽装

ネットワーク上で通信を行う際には，IP パケットの送受信が行われる．このパケットの中には様々な情報が内蔵されており，送信元 IP アドレスもその一つである．IP パケットの構造においては，TCP のバージョン，ヘッダ長をはじめとした様々な情報を示すフィールドが存在し，その中に送信元 IP アドレスを示すフィールドが存在する．前項で述べたように，DNS amp 攻撃にあたり，ボットコンピュータから攻撃用 DNS サーバへ名前解決要求が送信される際にそのパケットの送信元 IP アドレスは被害者のものに偽装される．

2.2.2 攻撃パケットの増幅

攻撃用 DNS サーバに送信元 IP アドレスが偽装された名前解決要求が送信されることで，DNS サーバは被害者に対して DNS 応答パケットを送信してしまう．この際，攻撃者は被害を最大限大きなものにするために，DNS サーバに対し TXT レコードの登録などの動作を行う．攻撃者はまず、大容量の文字列を並べた TXT レコードをあらかじめ任意のドメイン上に定義し，任意のドメインを管理する DNS サーバにこの情報を記録させる。そして DNS amp 攻撃としてそのドメインの名前解決を要求させることで，元は 40Byte 前後であった名前解決要求パケットに対し，最大 4096Byte のレコードデータを送信させることが可能となる．攻撃者の動きを含めた DNS amp 攻撃の概要を図 4 に示す．この動作によって応答パケットは増幅され，更に複数の DNS サーバを用いることで倍増していく．一連の処理を複数台のボットコンピュータを用いた攻撃と組み合わせることによって，被害者へより大きな被害を与えている．

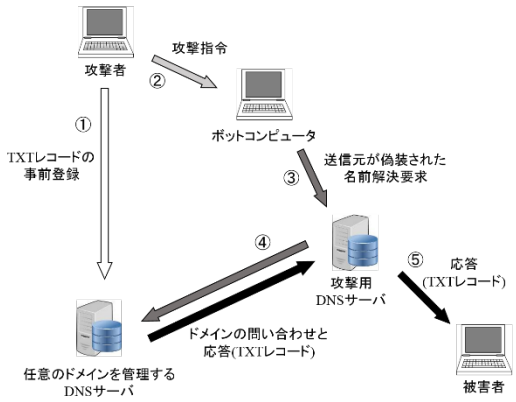

図 4: TXT レコードを利用した DNS amp 攻撃

3. 基盤技術および先行研究

本章では，DNS amp 攻撃への対策としての既存の技術と先行研究について，DNS サーバ側が施すもの，被害者側が施すものそれぞれについて述べる．その後，提案手法の研究課題を示す．

3.1 DNS サーバ側の対策

DNS amp 攻撃への対策としてまず挙げられるのが，DNS サーバが増幅器として利用されることを防ぐものである．これは攻撃が発生する前に予防として用いられる手法であり，その中でもキャッシュ DNS サーバに施すものと，権威 DNS サーバに施すものが存在する．以下，それぞれの対策に関して述べる．

3.1.1 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などが存在する．アクセスコントロールは送信元検証(Source Address Validation)という名称で RFC 2827/BCP 38 [5]，また RFC 3704/BCP 84 [6]に記されており，キャッシュ DNS サーバ側の設定によって，キャッシュ DNS サーバから自身が管理しないネットワーク空間に属する被害者へと送信される応答が破棄される．これにより，該当のキャッシュ DNS サーバが DNS amp 攻撃の踏み台として外部への攻撃に利用されるリスクが軽減される．ルータによるパケットフィルタリングでは，経路となるルータに送信元 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施し，該当パケットの通過を阻止することで攻撃を未然に防ぐ．

3.1.2 権威 DNS サーバにおける対策

権威 DNS サーバに関しては，キャッシュ DNS サーバに

おける状況とは大きく異なる. 権威 DNS サーバが名前解決要求を受ける際, その送信元はキャッシュ DNS サーバである. また権威 DNS サーバはインターネット全体に広くサービスを提供しており，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を行った場合には不都合が生じる．ボットコンピュータなどが利用され広範囲に存在するキャッシュ DNS サーバから大量の問い合わせを受けた場合，対応することができない．そのため，まず権威 DNS サーバが不必要な再帰検索要求の受付を拒否する設定を施す必要が存在する. そして権威 DNS サーバにおいて DNS の問い合わせそのものを制限するのではなく，DNS サーバの応答頻度を制限するための技術として，Paul Vixie らによって DNS RRL (DNS Response Rate Limiting) [7] が提案された．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，パケットの送信を中断し破棄する．DNS RRL を適用する上での問題点としては，統計的に攻撃の判断を行うため，本来正常であるはずの通信を中断してしまう事態など誤検出の発生が挙げられる．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[8]. 留意しなければならない点として, DNS RRL の適用はあくまで攻撃の被害を緩和するためのものである．そのため，複数のキャッシュ DNS サーバを用いられた場合には対処することができず，また各種問い合わせの間隔が設定された数値以上に開いていれば応答を返してしまう．

3.2 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，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 の適用であるが，こちらに関しても攻撃に利用されるネットワーク，DNS サーバの管理者が対策を施さない限りは影響を及ぼさない．そのため，被害者を保護するためには，回線の管理者や直接の被害者側による自衛手段として DNS amp 攻撃への対策が求められることになる. 被害者側を守る技術の一つが，被害者側のネットワークで行うフィルタリングである．このフィルタリングの先行研究として，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[9]．この手法では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．DDAA が保持するデータベースには通過するパケットの IP アドレス，宛先ポートなどの情報が記載される．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破棄する．

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 に高い負荷がかかりパフォーマンスに影響を及ぼす．そこで，Paola らによって機器に低負荷な手法が提案されている[10]．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，機器にかかる負担が軽減さる．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．

3.3 研究課題

DNS サーバ側の対策に関しては, DNS サーバの提供者に十分な知識と有効な対策の運用が求められ，一度発生してしまった DNS amp 攻撃に対し働きかけることが不可能である．したがって，被害者側にとっては DNS amp 攻撃に対し最善の対策であるとはいえない．そのため本研究の対象を被害者側の対策，中でも攻撃に対して直接的に作用するフィルタリング手法に設定する．被害者側の対策手法として, Ye らによって提案された被害者側のネットワークで行われるフィルタリング手法，また Paola らによる低負荷な手法を挙げた．しかしこれらの手法では，フィルタリングを行う端末にかかる負荷が大きく，またネットワークに影響が出るほど大規模な攻撃が行われた場合それに対応することができない．そのためパケットロスなどの障害を抑えられない．

そこで本稿では，フィルタリング端末の負荷の軽減，ネットワーク回線の負荷の軽減の 2 点を研究課題と設定し，パケットロスを防ぎ通信の可用性を守ることを目的としたフィルタリング手法を提案する．

4. 提案手法

本章では, 本研究が対象とする DNS amp 攻撃が実行される上で想定されるネットワーク環境と，それを踏まえた提

案手法を示す.

4.1 想定環境

本研究では, インターネットにおける自律システム(以下AS)内で OSPF が適用されていることを前提とする. 本節でこれらの紹介を行い，また提案手法での想定環境における端末について述べる.

4.1.1 Autonomous System

AS は大規模な TCP/IP ネットワークにおいて，ISP などの各組織がそれぞれ保有し，運用しているネットワークシステムのことである．インターネットは，複数の AS が相互に接続された形で表すことができる．AS はそれぞれに即したプロトコルが設定されており，それに基づき経路制御などの管理が行われている.

4.1.2 Open Shortest Path First

OSPF はリンクステート型と呼ばれ，AS の一種である．ネットワーク内で各ルータがどのように隣接するかというリンクステート(接続情報)を元に経路を選択する．ルータなどの通信機器が各通信機器間で経路情報を割り出し，ある地点から目的の地点に至るまでの最短経路を割り出す．ルータが保持した経路情報のデータベースを用いて各宛先への最短経路を割り出し，ルーティングテーブルを作成する．自身を含む全ての隣接ルータが同一エリア内に含まれる内部ルータ(Internal Router)，複数のエリアのルータと隣接するエリア境界ルータ(Area Border Router), 他の AS や異なるルーティングプロトコルで運用されているルータと隣接する AS 境界ルータ(Autonomous System Boundary Router)の 3 種類が存在する.

OSPF における最短経路の決定要因としては，主に機器間の帯域幅が用いられる．ネットワークでは通信速度の異なる回線が混在しているため，機器の数を用いた優先度よりも効率的にパケットを伝送することが可能である．それぞれのリンクを通過する際のコストを定量的に評価し，その値を用いて優先度を決定する.

4.1.3 提案手法における想定端末

提案手法では，DNS サーバから送信された DNS amp 攻撃パケットが，OSPF のエリアを通過することを想定する．攻撃パケットは AS 境界ルータを通過した後複数の内部ルータ, エリア境界ルータを経て被害者直近の内部ルータ(エッジルータ)に到達，その後被害者が管理する LAN ルータを経て被害者の端末に届くとする．この時，被害者の属する AS 外の通信に関しては考慮しないものとする．提案手法で用いるものの内, 新たに設置, 置換するもの以外では，AS 境界ルータ，内部ルータ，エリア境界ルータ，エッジルータ，LAN ルータ，被害端末が存在していることを想定する．しかし，LAN ルータより上流の端末において重要となるのは各ルータの役割そのものではない．そのため，以後それぞれのルータについて述べる際は特筆すべき理由が存在しない限りルータと表記する.

4.2 基本方針

提案手法では，攻撃が発覚し対応が決定された後に，複数のフィルタリングルータを用いて攻撃パケットのフィルタリングを行うことでアプローチを行う．またそれにあたり，攻撃発生時点で用いられていた経路，ルータとは異なる経路，ルータを用いる．複数本の経路，複数台のフィルタリングルータを利用することにより，ネットワークへの被害，ルータの処理量の低減を図る．また，一般にネットワーク回線は上流であればあるほど，帯域が広く設定されている．もし攻撃の規模が非常に大きいものとなり，経路の分散が行われる時点でネットワークへの悪影響が存在していた場合は，さらに上流に遡り，帯域に余裕のある地点から複数台によるフィルタリングを開始させる．この提案手法によって，既存の手法におけるフィルタリング端末への負荷の一極化，ネットワーク帯域の問題などによるパケットロスの問題の解決が見込める.

4.3 経路の分散と複数端末によるフィルタリング

本節では，提案手法の特徴である複数経路，複数端末を用いたフィルタリングについて述べる．経路の分散と複数のフィルタリングルータによるフィルタリングそれぞれの動作をまとめる.

4.3.1 経路の分散

攻撃が行われている環境下で攻撃が発覚した場合，あらかじめ開始用端末として設定されていた任意のルータに対し管理者からフィルタリングの開始が命令される．命令を受けたルータは攻撃経路上の 2hop 前の端末に対しフィルタリング動作を開始させる旨の通知を送信する．この通知を受信したルータは，被害者までの経路について，OSPF における次善の経路を求め，これまで用いてきた最短経路のルータと求めた経路のルータに対しフィルタリング動作を行わせる通知を送信する．各フィルタリングルータから応答が帰ってきたならば，フィルタリングに要する情報を送信し，受領した旨の通知が送信された後に経路を複数に分散させる．経路の分散について図 5 に示す.

Vol.2016-DPS-166 No.26
Vol.2016-CSEC-72 No.26
2016/3/4

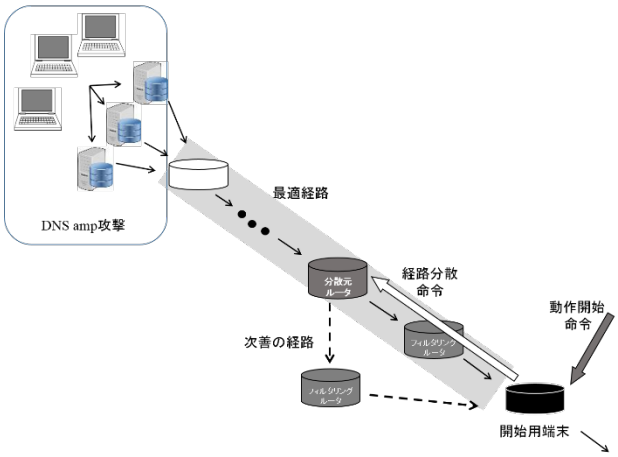

図 5: 通知による経路の分散

分散元ルータが経路の分散を行った後は，一定の間隔でパケットの送信先を切り替える．

4.3.2 複数端末によるフィルタリング

各ルータは自らに送信されたパケットに対しフィルタリングを施す．フィルタリングに用いる情報としては第一に，通過するパケットが DNS 応答パケットの特徴である UDP53 番ポート宛になっていることである．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くる 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 アドレスの情報を用いてフィルタリングを行う．その際，その DNS サーバの情報は分散元ルータを経由して同時にフィルタリング動作を行っているフィルタリングルータにも伝送し，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破棄する．

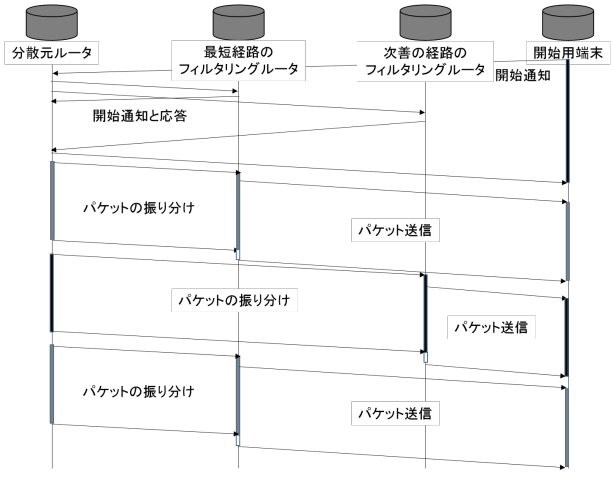

図 65: 動作開始からの各端末の動き

分散フィルタリングで，パケットの順序制御が重要である．次善の経路と最短経路を併用することでパケットの順序が入れ替わってしまい，パケットロスに繋がる．これを避けるために，各フィルタリングルータは，フィルタリングを終えたパケットを一定の期間バッファに保存してから送信する必要がある．開始用端末から分散元ルータに通知が送信されて以降の動きを図 6 に示す．

4.3.3 ネットワーク帯域に問題が生じている場合

輻輳の原因が振り分けを行う以前のネットワーク帯域の限界によるものであった場合，提案手法を用いてもネットワークへの被害を軽減することはできない．帯域の限界によって輻輳が発生した場合には，更にネットワーク回線を上流に遡らせて同様に複数ルータを用いたフィルタリングを行わせることで対応できる．

5. 実験と評価

本章では，提案手法の有効性を示すために行った実験及びその結果，既存手法と比較しての評価に関して述べる．

5.1 実験環境

本研究では，攻撃環境および提案手法をネットワークシミュレータ ns-3 上に実装した．実験ではシミュレーションシナリオとして，OSPF が適用された AS 内で DNS amp 攻撃を擬似的に再現した．特定の端末から DNS 応答パケットとして TXT レコードを連続的に送信させ，その上で各種測定用端末に被害端末との間で TCP 通信を行わせた．用いたパラメータを表 1 に示す．また，端末，リンクの概略図を図 7 に示す．

表 1: シミュレーションパラメータ
Table 1: Simulation Parameters

シミュレーション時間	90 [second]
最短経路内に存在するルータ数	5
最短経路を構成するリンク帯域幅	10-100 Mbps
次善の経路内に存在するルータ数	5
次善の経路を構成するリンク帯域幅	10-80 Mbps
攻撃用端末数	5
攻撃用端末が 1 秒あたりに送信するパケット最大数	2000
攻撃パケットの宛先ポート	UDP53

Vol.2016-DPS-166 No.26
Vol.2016-CSEC-72 No.26
2016/3/4

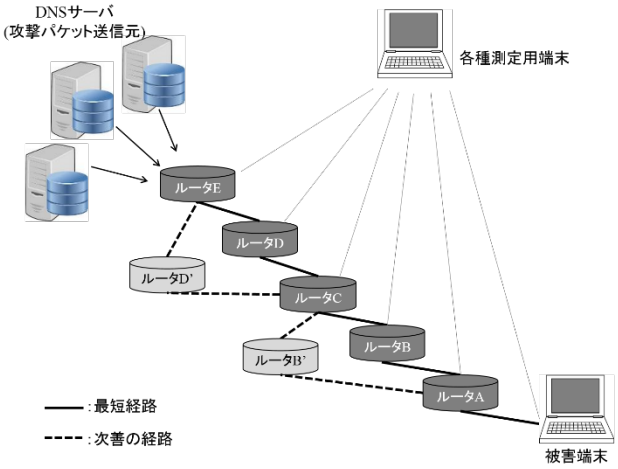

図 7: 実験におけるネットワーク構成

攻撃が行われた際の DNS サーバの再現を目的として設置した端末から，被害端末に向けて大量のパケットが送信させる．図 7 では，OSPF に従い最短経路を通って被害端末へと送信される．また各リンクに関しては，実験内容と被害端末からの距離によって帯域幅を変更している．ルータ A, ルータ C が提案手法における開始用ルータにあたる．また，単体フィルタリングはルータ A，ルータ C で行われているものとする．

5.2 評価内容

実験では，評価内容としてそれぞれ基準とするルータで分散フィルタリングを行わせた際の，分散元ルータから開始用ルータまでのスループット，パケットロス率を求め，またオーバーヘッドの定量的な評価としてフィルタリングによる攻撃パケットのブロック率，元々の通信で用いられるもの以外でやり取りが行われたパケット数を算出する．評価内容は，フィルタリング端末間のスループット，フィルタリング端末でのパケットロス発生率，フィルタリングによる攻撃パケットのブロック率である．これらの情報に関して，既存の手法である単体フィルタリングと比較，評価を行う．既存手法としては通過する端末に直接フィルタリングを行わせた場合のものを用いる．

5.3 実験結果

ここでは，前項で示した評価内容に関して，複数のシナリオを用いて実験を行った結果を述べる．

5.3.1 フィルタリング端末間のスループット

フィルタリング実行中の実行端末間のスループットについて，TCP プロトコルを用いて測定を行った．攻撃パケットの総量が少ない場合と多い場合，両方のスループットに関して，既存の単体フィルタリングを行った場合と分散フィルタリングを行った場合を測定し比較した．使用したパラメータを表 2 に示す．また図 8 に結果を示す．

表 2: 測定に用いたパラメータ

	攻撃パケット少	攻撃パケット多
秒間攻撃パケット数	500	5000
開始/フィルタリング用ルータ	ルータ A	ルータ C

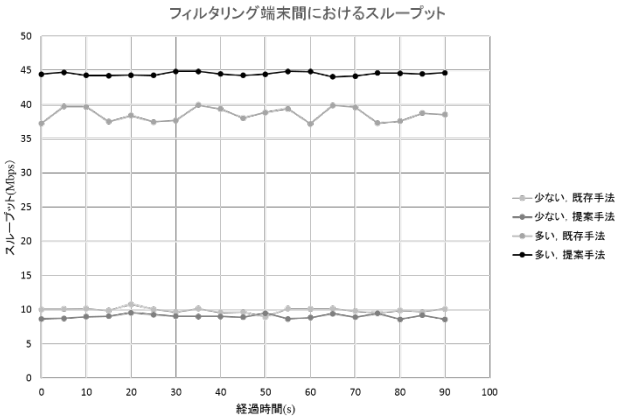

図 8: 攻撃規模ごとのフィルタリング端末間におけるスループット

図 8 に見られるように，攻撃パケットが少ない，すなわちフィルタリングを行う端末，またはネットワーク回線の帯域に余裕がある場合には大きな差は存在せず，既存の単体フィルタリング手法の方が安定して上回る結果を見せた．これはパケットの分散とフィルタリング後のバッファの存在により，通信の速度に影響が出たためであると考えられる．しかし攻撃パケットが多くなった場合は逆に，既存手法と比較して提案手法が明確に優位性を見せる．平均しておよそ 6.5Mbps もの差が生じた．

5.3.2 パケットロス発生率

次に, 前節の表 2 と同じパラメータを用いて実験を行い，フィルタリング端末前後でのパケットロスの発生確率を算出した．結果を図 9 に示す．

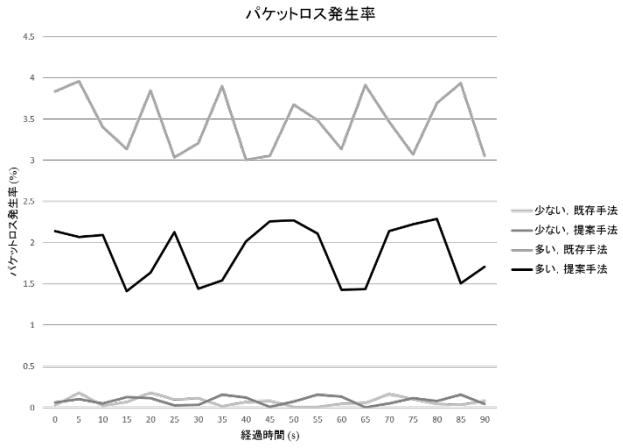

図 9: 攻撃規模ごとのパケットロスの発生率

パケットロスの発生率についてもスループットとほぼ同様の結果が得られた．攻撃パケットが少ない場合パケットロスはほぼ発生しないが，攻撃パケットの数が増加した場合は一定の値を示すこととなった．しかし提案手法を用いることで，既存手法と比較してパケットロス発生率がおよそ半分に抑えられている．被害を軽減することに成功しているといえる．

5.3.3 フィルタリングによる攻撃パケットのブロック率

続いて，フィルタリングを行った際の攻撃パケットのブロック率を示す．攻撃パケットのブロック率とは，攻撃パケットの内，フィルタリングによって破棄したパケットの割合を表す．結果を表 3 に示す．

表 3: フィルタリングによる攻撃パケットのブロック率

	既存手法	提案手法
攻撃パケット少	97.76	93.48
攻撃パケット多	94.48	92.29

攻撃パケットのブロック率に関しては，既存の単体フィルタリングを用いた方が良い結果が出た．これは既存の手法では単一の端末でデータベースの処理を全て行うことができ，対して提案手法では 2 つのフィルタリング端末が互いにデータベースを保持し，得られたデータが分散元ルータを経由させることで共有されるためであると考えられる．このためタイムラグや情報の齟齬が生じ，ブロックできないパケットが増加しているといえる．

6. 考察

実験結果から，提案手法は既存の単一の端末でフィルタリングを行う手法と比較して，攻撃規模が大きくなるほどスループット，パケットロス発生率の観点から優位性が生まれることが判明した．特にパケットロス発生率に関しては，単一の端末によるフィルタリングのパケットロス発生率がおよそ半分になり，明確にパケットロスのリスクが軽減されたとわかる．また，フィルタリング処理を行う端末が複数になったことから，フィルタリング動作において一台あたりの処理量が減少していることは自明である．これらの結果から，提案手法は研究課題を達成していると言える．しかしその反面，複数端末を用いることによって処理が煩雑化し，攻撃パケットのブロック率が低下した．今後は通知の効率的な受け渡しやバッファ時間の調整など，各端末の動作の最適化が求められる．本提案手法は，フィルタリングという動作の特性上，DNS amp 攻撃のみならず，様々な攻撃に対応することが可能である．今後の展望としては，異なる種類の攻撃に対処するための手法の考案などが考えられる．

7. 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．実験により提案手法を用いることによる利点を示し，既存手法と比較した際の優位性を示すことができたが，処理の最適化や複数種類の攻撃への対応などの課題が残される．

参考文献

1) Kaspersky Lab, “DENIAL OF SERVICE: HOW BUSINESSES EVALUATE THE THREAT OF DDOS ATTACKS,” IT SECURITY RISKS SPECIAL REPORT SERIES, https://press.kaspersky.com/files/2015/09/IT_Risks_Survey_Report_Threat_of_DDoS_Attacks.pdf, 2015.
2) Mockapetris P., “DOMAIN NAMES – CONCEPTS AND FACILITIES,” RFC 1034, 1987.
3) Mockapetris P., “DOMAIN NAMES – IMPLEMENTATION AND SPECIFICATION,” RFC 1035, 1987.
4) Damas, J., and Neves, F., “Preventing Use of Recursive Nameservers in Reflector Attacks,” RFC 5358, BCP 140, 2008.
5) Ferguson, P., and Senie, D., “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing,” RFC 2827, BCP 38, 2000.
6) Baker, F., and Savola, P., “Ingress Filtering for Multihomed Networks,” RFC 3704, BCP84, 2004.
7) Vixie, P., and Schryver, V., “DNS Response Rate Limiting (DNS RRL),” ISC-TN-2012-1-Draft1, 2012.
8) Rozekrans, T., and Koning, J., “Defending against DNS reflection amplification attacks,” University of Amsterdam System & Network Engineering RP1, 2013.
9) 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.
10) 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.