5R-02

マルチホーミングにおける IP アドレスホッピングを用いた DDoS 攻撃防御方式

岩永崇裕† 木村成伴‡

筑波大学 情報学群 情報メディア創成学類† 筑波大学 システム情報系 情報工学域‡

1. はじめに

インターネットセキュリティへの脅威として DDoS 攻撃の存在が挙げられる．DDoS 攻撃をうけたサーバは，許容量を超えた要求によりメモリや CPU，リンクの帯域といったリソースを食いつぶされ，正規ユーザに対して平常のサービスを提供できなくなる．DDoS 攻撃は一般的に防御が困難とされており，その理由の一つに，IP Spoofing を用いた攻撃が挙げられる．これにより，サーバ側は攻撃を仕掛けているノードを特定できないため，攻撃を防ぐことが難しい．これを踏まえて，IP Spoofing に強い DDoS 攻撃への防御策の必要性が高まってきている．

そこで，Khor らは，Overfort を提案している[1]．この方式では，サーバはマルチホーミングしており，通常は，一方の IP アドレスからのみ接続を受け付ける．攻撃時には，前者の IP アドレスでの接続は放棄し，秘匿していた後者の IP アドレスでのトンネリング接続のみ受け付けるが，攻撃者がサーバの名前解決に利用する LDNS（Local DNS）サーバに，トンネルの入り口の IP アドレスを通知しないペナルティを与えることで，攻撃トラフィックを送付できなくしている．しかし，この方式では，ISP が対応するゲートウェイを導入する必要があるなどの問題があった．

2. 提案方式

そこで本論文では，Overfort の，攻撃者が利用する LDNS にサーバの IP アドレスを通知しないというアイデアを用い，また，サーバサイドのみの実装で実現でき，かつ，IP アドレスが 1 つ漏えいしても破綻しない防御方式を提案する．

提案方式のネットワーク構成を，図 1 に示す．サーバサイドは，マルチホーミングしており，それぞれのサブネットに対してサーバのアドレスを複数個持たせる．図 1 の例ではマルチホーミング先は 2 つである．また，サーバサイドはいずれか 1 つのサブネットのみからパケットを受け取る設定（以下，アクティブ設定と呼ぶ）にしておき，それ以外のサブネットに届いたパケットは破棄する設定（以下，スタンバイ設定と呼ぶ）にしておく．また，サーバの権威 DNS（以下，ADNS）は，例えば，図 2 に示すようなアドレス通知テーブルを持ち，LDNS など，問い合わせを行ってきた相手の IP アドレスに応じて，通知 IP アドレス（図では IPA1～IPA3）を変更する．

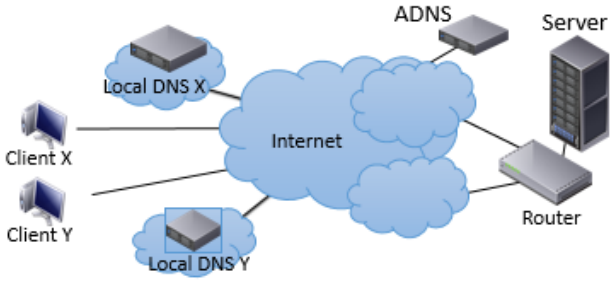

図 1．提案方式のアーキテクチャ

LDNSのアドレス	0.0.0.0～ 73.255.255.255	74.0.0.0～ 146.255.255.255	147.0.0.0～ 223.255.255.255
通知IPアドレス	IPA1	IPA2	IPA3

図 2．アドレス通知テーブルの例

攻撃検出法については他の提案方式を利用し，攻撃検出後は，これまでスタンバイ状態だったサブネットの 1 つをアクティブ設定に，攻撃を受けているアクティブ設定のサブネットをスタンバイ設定にする．さらに，ADNS のアドレス通知テーブルの通知する IP アドレスをアクティブ設定にしたサブネットの IP アドレスにし，通知先の LDNS のアドレスの範囲をずらす．ここで，攻撃時にサーバの IP アドレスを変更する一連の処理を IP アドレスホッピング（以下 AH）と呼ぶ．

通知するアドレス範囲をずらす理由は，2 つある．1 つは全てのアドレスに対して平均的に攻撃を仕掛けるなどの，計画的な攻撃をしにくくするためであり，もう一つは，変更後の IP アドレスに追従して攻撃が行われる場合，AH を何度か繰り返すことで，攻撃者が利用する LDNS を絞り込んでいくためである．これにより，攻撃者が利用する LDNS を含む IP アドレスの範囲の LDNS 群には，AH 前のアドレスを通知し続けるペナルティを与える．AH 前のアドレスが属するサブネットはスタンバイ設定をしており，ここに到達したパケットを破棄するが，攻撃者からは DDoS 攻撃が成功しているように見えるので，防御機

A DDoS Attack Defense Method Using IP Address-hopping on Multihoming
†Takahiro Iwanaga, School of Informatics, College of Media Arts, Science and Technology, University of Tsukuba
‡Shigetomo Kimura, Faculty of Engineering, Information and Systems, University of Tsukuba

構が働いていることに気づきにくいと考えられる．なお，AH を行ってもまだ攻撃を検出した場合は，可能な限り AH を繰り返すこととする．

3. 実験

提案方式の有効性を確認するため，本章ではシミュレーション実験を行う．本実験において，TCP のサービスを提供するサーバがあり，攻撃者は，サーバに至るリンクを攻撃する UDP Flooding を行う．そして，本提案方式を用いる前と用いた後における，正規ユーザのスループットなどを観測する．

攻撃ノード(Attacker)が用いる，サーバの名前解決手段として，(1)Attacker がそれぞれ名前解決を行う，(2)正規ユーザを装うノード(Faker)がアクセスできた名前解決結果を Attacker が用いる，(3)Zombie マスタなどの単一ノードが名前解決した結果を Attacker が用いる，の 3 種類を想定し，その各々について，(A)攻撃中も再度の名前解決を行う場合，(B)一度名前解決した結果を継続して使い続ける場合，の計 6 通りによるシミュレーションを行った．また，攻撃検出後は，各 LDNS 範囲の合計スループットを算出し，それらの平均＋標準偏差よりも大きいスループットの範囲に属する LDNS にペナルティを与える．実験のシミュレータには ns-3 を用いた．実験トポロジと各ノードの設定を図 3 に示す．

ノード	データレート	プロトコル	ノード数
Attacker	20Mbps	UDP	6
User	4Mbps	TCP	9
Faker	4Mbps	TCP	3

各リンクの帯域:100Mbps
マルチホーミング数:3
サーバアドレス数:I/Fごとに4,8,16で実験

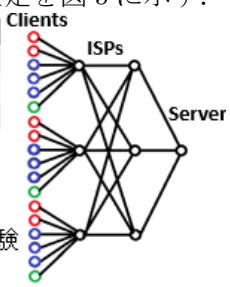

図 3. 実験設定

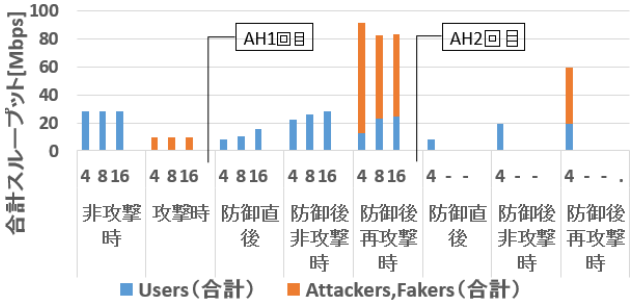

図 4. 攻撃法(1)(A)に対する防御

なお，各ノードの IP アドレスはランダムに決定し，それぞれのサブネットは重複しないものとする．また，各ノードは，そのサブネット内にある LDNS を利用するものとし，OpenDNS などの公開 DNS キャッシュサーバは用いないものとする．

図 4 に，攻撃法(1)(A)の場合の，正規ユーザ，Attacker/Faker 別の，平均合計スループットの時間的推移（DNS キャッシュ有効時間(10 秒)間隔）を，サーバの I/F ごとのアドレス数別に示す．

攻撃時は，正規ユーザの平均合計スループットがほぼ 0 になり，攻撃側（Attacker/Faker）のそれも，パケットロスにより，およそ 9.5Mbps になった．1 回目の AH 直後，攻撃側の平均合計スループットは 0 となり，正規ユーザのそれは，8.09～15.68Mbps，それからキャッシュ有効時間経過後には 22.56～28.58Mbps に回復する．しかし，その 10 秒後に攻撃者がサーバのアドレス変更に追従し，変更後のアドレスに再攻撃すると想定した次の間隔では，各 I/F ごとのアドレス数が 4 の場合は，攻撃側へのペナルティが十分ではなく，攻撃側の平均合計スループットは 79.22Mbps，正規ユーザのそれは 12.26Mbps となって，非攻撃時並の平均合計スループットを確保するには，もう一度，AH を行わなくてはならなかった．これに対して，各 I/F におけるアドレス数が 8 および 16 の場合は，2 回目の攻撃側の平均合計スループットは 59.45Mbps 程度だが，正規ユーザのそれは，24.25Mbps 程度となり，非攻撃時と同程度の平均合計スループットを確保できている．このことから，1 回の AH で十分なペナルティが与えられ，DDoS 攻撃が防御できたと言える．

他の攻撃法についても，各 I/F におけるアドレス数が 8，16 の場合は，2 回（＝マルチホーミング数－1，以下限界 AH 回数と呼ぶ）内で全て防御可能であった．アドレス数が 4 の場合は，攻撃法(2)(A)を除き，限界 AH 回数内で防御可能だった．

なお，サーバの I/F ごとのアドレス数が多いほど，正規ノードがペナルティを受ける割合が減ることもわかった．また，正規ユーザを装うノードが，攻撃者に利用可能なアドレスを通知する攻撃法では，比較的多くのアドレスホッピング数を要することがわかった．さらに，攻撃中，再度の名前解決を行わない攻撃では，AH1 回で攻撃ノードが 100%分離できることが確認された．

4. まとめ

本論文では，IP アドレスホッピングを用いて IP Spoofing された DDoS 攻撃に対する防御方式を提案した．今後は UDP Flooding 以外の攻撃に対する実証実験や，公開 DNS キャッシュサーバが用いられた場合の対処法などを検討していきたい．

参考文献

[1] Soon Hin Khor and Akihiro Nakao, “Overfort: Combating DDoS with Peer-to-peer DDoS Puzzle,” Proceedings of IEEE International Symposium on Parallel and Distributed Processing, pp. 1–8, 2008.