2Y-5

DDoS 攻撃の為の送信元識別子を用いたフィルタリング方式

井熊一博† 木村成伴‡ 海老原義彦‡
筑波大学情報学群情報メディア創成学類†
筑波大学大学院システム情報工学研究科‡

はじめに

インタネットの普及に伴い，様々なネットワークサービスが提供されており，サービス事業者はそれらのサービスを継続的に運用することが求められている．その障害となるものの一つに DDoS (Distributed Denial of Service)攻撃がある．この攻撃は，ネットワーク上で分散した地点に接続された多数の攻撃者が，攻撃対象へ一斉に大量のパケット（以下，攻撃パケット）を送信することで，攻撃対象が提供するサービスの継続を困難にさせるものである．攻撃者は正規ユーザを装った攻撃パケットを送信するため，正規ユーザのパケット（以下，正規パケット）と攻撃パケットを区別する事は難しい．

この問題を解決する方法の一つとして Pi (Path Identification)方式が提案されている[1]．この方式では，各ルータにおいて，自分が中継するパケットに自分の識別子（IP アドレスの一部など）をマーキングする．これにより，受信側はパケットが通過したおおよその経路を知ることができる．そして，同じマーキングを持ち，単位時間当たりの送信量が極端に大きいパケットを遮断することで，DDoS 攻撃を防御する．しかし，マーキングできるビット数が限られるため，経路が途中から一致する正規パケットと攻撃パケットのマーキングが同じになり，これらが区別できなくなるという問題があった．

提案方式

Pi 方式の問題点を解決する為，我々の研究室では，Pi 方式の識別子とプロトコル番号などを併用する方式[2]や，Pi 方式と Pushback 方式と組み合わせた方式[3]を提案している．しかし，前者は正規パケットと攻撃パケットの区別が十分ではなく，後者はルータに Pushback 方式を導入するため，実装がより複雑になるという問題があった．そこで本論文では，送信者から送られたパケットが最初に届いた（WAN 側の）ルータで，パケットの送信者の MAC アドレスをマーキングし，送信元を識別することで DDoS 攻撃を防御する方式を提案する．MAC アドレスは，ネットワークインタフェースに一意に割り当てられている値だが，このアドレスはソフトウェアでフレームヘッダに書き込まれる為，偽装することが可能である．しかし，送信元 MAC アドレスとしてランダムな値を用いて大量のパケットを送付すると，LAN 内に異常に多くの通信機器があると認識されることから，ルータが異常を検知できる．この為，送信元 IP アドレスに比べ，送信元 MAC アドレスの偽装は少ないと考えられる．

但し，攻撃者が送信元 MAC アドレスを特定の値に偽装すると，これと同じ MAC アドレスを持つ正規ユーザのパケットもフィルタリングしてしまう可能性がある．そこで提案方式では，送信者の MAC アドレスに加えて，最初のルータがパケットを受け取った時の TTL の値をマーキングする．これにより，到着時の TTL との差を求めることで，途中のルータが提案方式をサポートしていなくても，最初のルータから何ホップ中継されてきたかが分かる．このため，送信元 MAC アドレスを偽装した攻撃パケットと正規パケットを区別できる確率が高くなると期待される．

最後に，受信側は MAC アドレスとホップ数毎に単位時間当たりの送信量を求め，これが多いパケットは DDoS 攻撃と判断して破棄する．

シミュレーション実験

提案方式の有効性を確認する為に，ネットワークシミュレータ NS2 を用いてシミュレーション実験を行う．正規ノードと攻撃ノードの送信内容を表 1 に，実験で用いたネットワークのトポロジを図 1 に示す．ここで，ノード間の回線の帯域は 100Mbps，伝搬遅延は 2 ミリ秒である．

図 1 で，正規パケットを送るのは正規ノードの S1 と S2，攻撃パケットを送るのは攻撃ノードの A1，A2 ,A3 である．固定の転送速度で，攻撃

表 1：正規ノードと攻撃ノードの送信内容

A Filtering Method by Source Identifications against DDoS Attacks

†Kazuhiro Ikuma, College of Media Arts, Science and Technology, School of Informatics, University of Tsukuba
‡Shigetomo Kimura and Yoshihiko Ebihara, Graduate School of Systems and Information Engineering, University of Tsukuba

	正規ノード	攻撃ノード
プロトコル	ICMP	UDP
転送速度	1kbps	100Mbps
パケットサイズ	1024byte	210byte

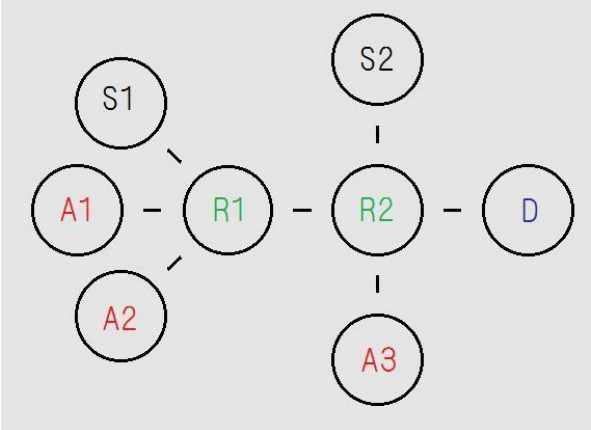

図 1：実験におけるトポロジ

ノードは UDP によるパケットを，正規ノードは ICMP エコー要求を送信し，その送信先はいずれも D である．R1 と R2 は提案方式を実装したルータであり，R1 は S1，A1，A2 が送ったパケットに，R2 は S2 と A3 が送ったパケットに，それぞれの MAC アドレスと TTL をマーキングする．D はこの MAC アドレスとホップ数毎に，過去 10 秒間の送信量から 1 秒当たりの送信量を求め，帯域の 30% 以上であれば攻撃ノードと見なした．

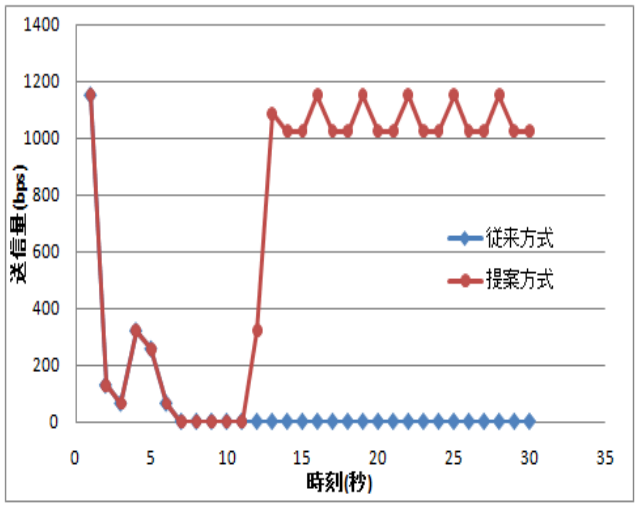

図 2：従来方式と提案方式における S1 から D へ到達したスループットの変化の様子

実験では，開始直後から 1 秒間は，正規ノードのみが送信を行い，その後，攻撃ノードが送信を開始する．これを合計 30 秒間行い，ルータで提案方式を有効にしなかった場合（以下，従来方式）と提案方式を有効にした場合における，S1 から D へ届いたパケットのスループットを 1 秒毎に求めた結果を図 2 に示す．

図 2 において，従来方式は実験開始から 1 秒後まで正常な通信ができているが，その後，攻撃ノードが攻撃を始めるとスループットが低下し始める．そして，約 7 秒後以降は 0bps となり，正常な通信が出来ていない状態に陥っている．

一方，提案方式においても，実験開始から 1 秒後までは正常な通信ができているが，その後，攻撃ノードが攻撃を始めると，従来方式と同様に，スループットが低下し始め，実験開始から 7 秒後から 11 秒後までは 0bps となっている．これは，攻撃を始めた直後から 10 秒間は送信量の実績を蓄積するため，この間は，攻撃パケットを受け取る必要があるからである．しかし，攻撃の実績が蓄積され，攻撃パケットを破棄し始めた 12 秒後には 320bps に，13 秒後以降は平均 1.063kbps になり，攻撃前の値まで回復することができた．以上の結果より，攻撃パケットを確実に破棄し，正規パケットを DDoS 攻撃の影響から回復できたことから，提案方式が有効であることが示された．

まとめ

DDoS 攻撃から防御するため，送信元識別子として送信元 MAC アドレスとホップ数を用いたフィルタリング方式を提案し，シミュレーション実験によりその有効性を示した．実験において，提案方式は，攻撃されてから元のスループットに回復するまで 10 秒以上を要している．これは，単位時間当たりの送信量を計算する為に過去 10 秒間の送信量を求めているためだが，今後，送信量の求める方法を調整する予定である．

参考文献

[1] Abraham Yaar, Adrian Perrig, and Dawn Song, “Pi: A Path Identification Mechanism to Defend against DDoS Attacks,” Proc. of the 2003 IEEE Symposium on Security and Privacy (SP'03), pp. 93–107, 2003.

[2] 志田雄哉, 木村成伴, 海老原義彦, “DDoS 攻撃のためのパス識別子メカニズムにおけるプロトコル単位でのフィルタリング方式の提案,” 情報処理学会第 68 回全国大会, 6R-8, pp. 3-673–3-674, 2005.

[3] 金子陽一, 木村成伴, 海老原義彦, “Pi 方式と Pushback 方式を組み合わせた DDoS 攻撃防御方式の評価,” 情報処理学会第 70 回全国大会, 1ZB-7, pp. 3-397–3-398, 2007.