6R-8

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

志田 雄哉† 木村 成伴‡ 海老原 義彦‡

筑波大学 第三学群情報学類† 筑波大学大学院 システム情報工学研究科‡

1．はじめに

近年，インターネットの急激な普及に伴い，各種ネットワークサービスは一般ユーザの生活にとって密接に関わるようになり，これらのサービスを継続的に提供することが重要になっている．その障害となるものの１つとして，DoS (Denial of Service)と呼ばれる外部からの攻撃がある．この攻撃は，一見すると正規ユーザからのものと思われるアクセスを装った大量のパケットを送付することにより，特定のサーバあるいはその周辺ネットワークをサービス不能状態に陥らせる手法である．また，この攻撃をネットワーク的に離れた位置にある複数のコンピュータから同時に行う DDoS (Distributed DoS) 攻撃も見受けられる．一般に，この DDoS 攻撃を防御するのは難しいとされており，この攻撃に対する防御方法の確立が急務になっている．

2．Pi (A Path Identification Mechanism)について

DDoS 攻撃を防御する方法は 2 種類に大別され，１つは攻撃対象となるサーバとその周辺ネットワークのみで防御する方式と，ネットワーク全体で協調することで防御する方式である．前者は後者よりも導入が容易という利点があるが，DDoS 攻撃に関する情報の取得が限られることから，後者の方がより柔軟性があるといえる．

後者の防御手法の１つとして Pi (A Path Identification Mechanism)[1] がある．Pi では，ネットワーク上のルータにおいてそこを通過するパケットに対してマーキングを行う．マーキング手法としては，転送するパケットの ToS フィールドなどに対して各ルータ自身の IP アドレスの末尾１，または２ビットを識別子として書き込む方法などが考えられている．

宛先ホストに到達した時点で，同一のマーキング値を持つパケットの送り元は同一だと判断する．そして，この値単位での到着パケット数の統計を取り，過剰に多いものについては攻撃パケットとみなしてこれを廃棄する．

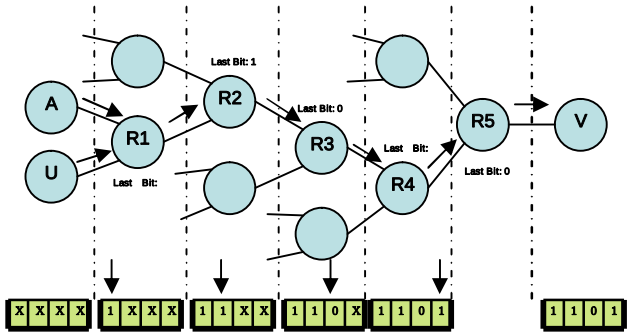

図１．Pi によるマーキング

図１の例では，攻撃者 A からのパケットはネットワーク上のルータ R1 から R5 を経由して攻撃対象 V に到達しており，ルータ R1 から R4 がこのパケットにマーキングした結果，この値は“1101”となった．なお，宛先近辺における経路の違いは送信元の推定に障害となることから，図１ではルータ R5 でのマーキングを行っていない．

3．提案方式

Pi 方式では，各ルータでのマーキングや各サーバでのフィルタリングに要する負荷が非常に低く，送付されたパケットが通過した経路の情

A Proposal of Filtering Methods Using Path Identification Mechanism Based on Protocol Numbers for DDoS Attacks

†Yuya Shida: College of Information Sciences, Third Cluster of Colleges, University of Tsukuba

‡Shigetomo Kimura and Yoshihiko Ebihara: Graduate School of Systems and Information Engineering, University of Tsukuba

報が得られることから，フィルタリングの精度が比較的高いと考えられる．しかし，図１の正規ユーザ U のように攻撃者 A と同じ経路を辿った場合や別な経路であってもマーキングの値が一致した場合，正規ユーザのパケットが攻撃者のパケットとして廃棄されるという問題がある．

これを解決するため，本論文では前章で述べた Pi によるフィルタリング方式を改良し，マーキングの値に加えて，パケットで用いているプロトコル単位での統計を取り，その頻度に応じて攻撃者かどうかを判別する．

ここで，プロトコルを識別するために幾つかの方法が考えられるが，提案方式では IP パケットのヘッダにあるプロトコル番号フィールドの値を用いることとする．図２に主なプロトコルに対して与えられるプロトコル番号を示す．

Decimal	Keyword	Protocol
1	ICMP	Internet Control Message Protocol
6	TCP	Transmission Control Protocol
17	UDP	User Datagram Protocol

図２．主要なプロトコル番号

例えば，攻撃者が ICMP エコー要求を用いた DDoS 攻撃を行っていたとする．Pi の手法では，正規ユーザによるパケットが攻撃者のそれと同じマーキング値を持つ限り，TCP や UDP などの ICMP 以外のプロトコルを用いていたとしても，それらのパケットはフィルタリングされていた．本提案方式を用いることで，これらの場合に正規ユーザのパケットはフィルタリングされなくなり，この点において正規ユーザと攻撃者の識別精度が上がったといえる．

なお，より細かい単位での分類を行うためには，例えば，TCP や UDP のポート番号や ICMP のタイプやコードなどを参照する方法が考えられる．これにより，正規ユーザと攻撃者の識別精度をより向上させることができる反面，これらの値を参照するための処理遅延が増加し，統計データを格納しておくためのメモリ容量が増大するといった問題がある．このように，識別精度と処理遅延がトレードオフの関係になっていることを踏まえ，提案方式では IP のプロトコル番号フィールドの値によるプロトコルの分類を採用した．

４．評価実験

前章の提案方式の有効性を評価するため，図３に示すネットワークを用いた通信実験を行う．ここで，攻撃者 A と正規ユーザ U1，U2 は攻撃対象 V に対して図に示すプロトコルを用いて通信を行う．この状況下において，攻撃対象 V で Pi または提案方式による手法のそれぞれを用いて DDoS 攻撃に対する防御を行ったとき，V が受信したパケットの送信者毎の受信率とこれに要した処理時間を比較する．これにより，攻撃者からの防御の精度と，それに対する正規ユーザへの影響を示すとともに，本提案方式の妥当性を検証する．

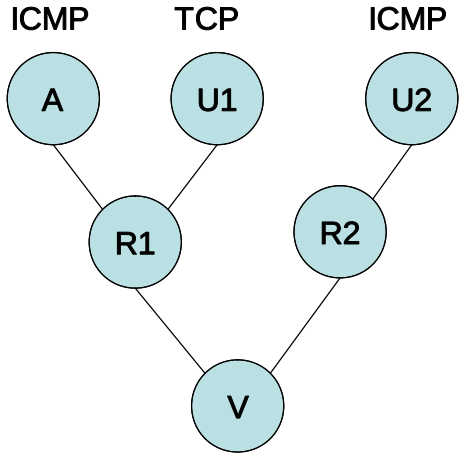

図３．評価実験用ネットワーク環境

５．まとめと今後の課題

本論文では，ネットワーク全体において DDoS 攻撃に対する防御を行う Pi に対して，新たにプロトコル単位でのフィルタリング方式を導入した．そして，本提案方式の有効性を確認するための評価実験についても述べた．

今回の実験では小規模なネットワークを用いて行ったが，Pi 及び本提案方式はネットワーク全体において防御策を講じる方式であり，より大規模なネットワークにおいて有効に働くことを示す必要がある．

参考文献

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