2W-08

ホップカウント初期推定値に基づく学習を用いたホップカウントフィルタリング方式

山越　寛† 　木村 成伴 ‡

筑波大学情報学群情報科学類† ‡ 筑波大学システム情報系情報工学域

1. はじめに

近年，サイバ攻撃が増加の一途を辿っている．DoS 攻撃に代表される悪意あるアクセスの多くは IP スプーフィングと呼ばれる送信元 IP アドレスを偽装する技術を使用している．IP スプーフィングを利用することで，攻撃者はフラッド攻撃元を隠してフラッドトラフィックの地域性を薄めたり，正当なホストにフラッドトラフィックをリダイレクトさせることでリフレクタ攻撃元として悪用したりすることが可能になる．そのため，スプーフィングされた IP パケットを検出して破棄することは，自身を防衛するだけでなく，攻撃者に加担してしまうことを防ぐためにも有効である．そこで，攻撃者は送信元 IP アドレスを偽装することはできても，IP パケットが目的地に達するまでのホップカウント(HC: Hop Count)を偽装することはできない事を利用し，Time to Live フィールド(TTL)の値から HC を推定し，送信元 IP アドレスとホップカウントのマッピングを使用することで，IP スプーフィングを検出するホップカウントフィルタリング(HCF: HC Filtering)が提案されている[1].

HCF では，まず，学習段階で送信元 IP アドレスと HC の対応を IP2HC マッピングテーブルに記録し，フィルタリング段階でテーブルの記録に合致しない送信元 IP アドレスと HC の組あわせをもつパケットを破棄する．しかし，この方式では，学習段階に攻撃を受けると，異常な送信元 IP アドレスと HC の対応を学習してしまう可能性がある．また，攻撃者に偽装する送信元の経路情報を把握されると，初期 TTL を偽装することでフィルタリングを回避できる．偽装パケットが少ない時は，学習段階からフィルタリング段階に遷移できないため，フィルタリングできなくなるなどの問題があった．

Hop Count Filtering Method with Hop Count Learning Based on Initial Estimate Value

Hiro Yamakoshi†, Shigetomo Kimura‡

†College of Information Science, School of Informatics, University of Tsukbua

‡Faculty of Engineering, Information and Systems, University of Tsukuba

これらのうち，学習段階における問題を解決するために，本論文方式では HCF の学習段階において，IP2HC マッピングテーブルに頼らないフィルタリングを行う方式を提案する．これにより，学習段階に攻撃を受けると，異常な送信元 IP アドレスと HC の対応を学習することを防ぐ．

2. HCF (Hop Count Filtering)

送信元がパケットに設定する TTL の初期値は任意だが，通常のアプリケーションでは，OS がデフォルトで設定する値を使う場合がほとんどである．そこで HCF では，TTL の初期値の候補を幾つか選択しておく．そして，到達したパケットの TTL よりも大きい TTL 初期値候補のうち，最も小さいものを TTL の初期値であると推定し，推定される TTL 初期値とパケットの TTL の差を HC として扱う．

HCF の実行状態には，学習段階とフィルタリング段階の 2 つの段階がある．学習段階に於いては，到着したパケットの送信元 IP アドレスと TTL から計算した HC の対応を IP2HC マッピングテーブルに保存する．この時，IP2HC マッピングテーブルの正当性を保つために TCP スリーウェイハンドシェイクの最後の ACK パケットで IP2HC テーブルを更新する．また IP2HC テーブルが膨大に成ることを防ぐために，クラスタリングを行う．このテーブル更新は TCP 処理のクリティカルパスで行われるため，管理者は更新頻度を設定できる．

但し，学習段階に於いては，偽装されていると判定されるパケットがあってもフィルタリングされることはなく，全てのパケットは HCF を通過するが，その数がある閾値を超えた時，HCF はフィルタリング段階に遷移する．フィルタリング段階では，到着した全てのパケットの送信元 IP アドレスと HC の対応が検査され，IP2HC テーブルと合致しない対応を持つパケットは全て破棄される．

さて，HCF を正常に稼働させるためには，事前にある程度の期間，送信元 IP アドレスと HC の対応を収集し，IP2HC マッピングテーブルを作成しなければならない．この収集期間はサーバに到達するトラフィック量に依存し，その収集期間

中は，HCF は全くの無防備である．特に，閾値を超える数のパケットが到達しない場合は，HCF はフィルタリング段階に入ることができず，無防備な学習状態を継続することになる．また，この期間に，ルーティングテーブルの一時的な変更に伴う迂回ルートを経由してきたパケットや攻撃者が意図した値を学習させようとするパケットの HC を正しい値として学習してしまう可能性がある．一方，フィルタリング段階に入ったとしても，traceroute 等によって，攻撃者が偽装する IP アドレスを持つホストと攻撃対象のサーバまでの間の HC を取得できた場合，攻撃するパケットの TTL 初期値を変えることで，HCF を回避できるという問題がある．

3. 提案方式

HCF の問題のうち，学習段階の問題を解決するため，提案方式では，HCF の学習段階において，IP2HC テーブルに頼らないフィルタリングを行う．一般に，HC は高々30 程度であることがほとんどである[2]．そこで，この値を HC の初期推定値とし，典型的な OS で用いられる TTL の初期値[3][4]である 60,64,128,255 よりも 30 以上減った TTL を持つパケットは異常であるとする．つまり，正当なパケットの到着時の TTL n は 30 ≦ n ≦64, 98 ≦ n ≦ 128, 225 ≦ n ≦ 255 の範囲に収まると判断する．そして，この範囲に収まる TTL のパケットについては，HCF と同様に学習して，IP2HC テーブルにマッピングを行うとともに，それ以外のパケットについては，異常なパケットであるとして，学習段階であっても破棄する．

この提案方式により，明らかに異常な HC を学習しないことで，IP2HC マッピングテーブルの健全性を保つことが出来る．また，TTL が 30 未満のパケットが破棄されるため，traceroute 等で用いられる ICMP エラーメッセージも破棄され，サーバへの経路特定を妨げることが出来る．さらに，従来の HCF では対応できない，少量の偽装パケットにも対応が可能になることも利点として挙げられる．

4. シミュレーション実験

本章では，ns3 を使用したシミュレーション実験を行い，提案方式の有効性を確認する．実験で用いるネットワークトポロジを図 4.1 に示す．

この図において，各端末とサーバが接続するリンクの帯域は 100Mbps である．正規ユーザも攻撃者もサーバと TCP で接続し，1024 バイトのパケットを，正規ユーザは 0.5s 間隔で，攻撃者は 0.1s 間隔で送信する．

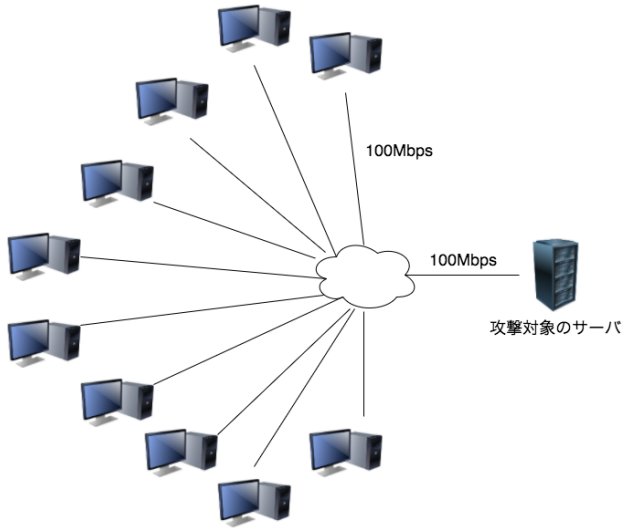

図 4.1 ネットワークトポロジ

以上の条件において，全ノードにしめる攻撃者の割合を変化させ，60 秒間通信した時の，従来方式と提案方式を用いたときの攻撃パケットがサーバに到達した割合を比較する．

5. まとめ

本論文では，HCF の学習段階において IP2HC テーブルに頼らずにフィルタリングを行うことで，学習段階が全くの無防備であった欠点を改善した．また，攻撃準備の事前調査活動の阻止や IP2HC マッピングテーブルの健全性を向上させた．今後，シミュレーションプログラムを完成させ，提案方式の有用性を確認する．

参考文献

[1] Haining Wang, Cheng Jin, and Kang G. Shin, “Defense Against Spoofed IP Traffic Using Hop-Count Filtering,” IEEE/ACM Transactions on Networking, Vol. 15, No. 1, pp. 40–53, 2007.

[2] K. Claffy, T. E. Monk, and D. McRobb, “Internet Tomography,” Nature, 1999.

[3] Swiss Academic & Research Network, “Default TTL Value in TCP/IP,” http://www.map.meteoswiss.ch/map-doc/ftp-probleme.htm (参照 2017/1/13).

[4] Default Time to Live (TTL) Values http://www.binbert.com/blog/2009/12/default-time-to-live-ttl-values/ (参照 2017/1/13).