エントロピーに基づく不正アクセスＩＰパケットの特徴抽出

○本田　秀一、中嶋　卓雄（九州東海大学）、小島　俊輔（八代工業高等専門学校）

1.　はじめに

コンピュータの利便性に反してセキュリティの確保が問題になっている。特にサーバに大量の不正なパケットを送りつける DoS(Denial of Service) 攻撃が頻繁に行われると、サービスの悪化、中断させるとともに、メモリーリソースを使い果たすだけではなくネットワークリソースも使い果たす可能性がある。その DoS 攻撃を検出するためにセキュリティポリシに基づいてのフィルタリングルールを構成するが、近年増加傾向にある DDoS（Distributed Denial of Service）攻撃の場合は攻撃者により不正プログラムをインストールされたボットと呼ばれる複数のホストからリモートで一斉に攻撃が行われるため、送信元ＩＰアドレスが特定しにくく、この単純なフィルタリング手法では攻撃を検出することが困難である。

本研究ではその DoS 攻撃の統計的特性を抽出し攻撃を早期に検出することを目的とする。

2.　統計指標

エントロピー(H)を以下のように定義する。

$$H = -\sum_{i=1}^{n} Pi \log_2 Pi \quad (1)$$

$$Pi = \frac{\text{送信元ＩＰアドレス}(i)\text{の頻度}}{\text{頻度の総数}} \quad (2)$$

この解析で i は一つの送信元 IP アドレスを意味しており、確率は送信元 IP アドレスの総数で割って得ることができる。スライディングウィンドウも使用しており、図１に例を示す。一定の時間幅を window として定義し、アクセス時間がその window 中にある送信元ＩＰアドレスごとに頻度をとり、全体頻度に対する確率をもとめ、エントロピーを計算する。 そして window を一定の時間幅でスライドさせることにより、エントロピーの時系列変化を得ることができる。この幅をスライディング幅と呼び、図１では W１、W2、W3 はそれぞれ１回目、２回目、３回目の window の場合、S がスライディング幅である。

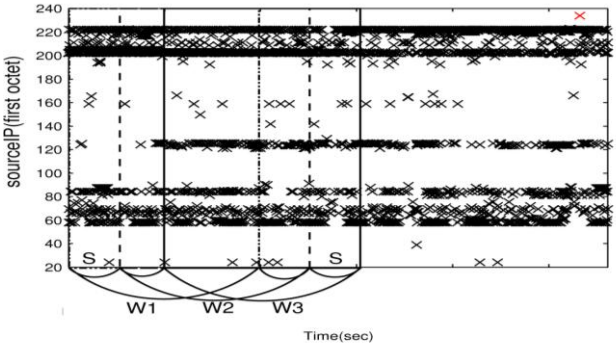

図１．スライディングウィンドウの例

このwindowサイズとスライディング幅は解析する際のデータの件数やアクセス時間の間隔によって適切な数値に調節する必要がある。

DDoS (Distributed Denial of Service) 攻撃は複数のホストからパケットが送信されるので通常のトラフィックとは異なり、送信元ＩＰアドレスが分散している特長があると考えられる。複数の送信元ＩＰアドレスからアクセスがあると情報量が増える。すなわちエントロピーの変化を時系列でグラフ化することにより DDoS 攻撃の始まりを検出することができる。

3.　実験環境

実験環境を図２に示す。この実験データは八代高等専門学校のエッジルータである Firewall でのフィルタリングデータを利用している。解析には Firewall の log-data を内部ネットワーク中にある Syslog Server にリアルタイムで転送したデータを使用する。FW は WAN 側からのアクセスは DMZ 以外すべて受け付けない設定になっている。また DMZ 内には Web サーバが設置してあり送信先ＩＰアドレスがサーバ以外の TCP80 番ポートへ向けたパケットは破棄する設定になっている。本研究では、この FW のフィルタリングルールにより破棄された TCP80 番ポートのデータに基づいて、そのパケットの送信元 IP アドレスとアクセス時間を抽出して解析する。データは 2007 年４月 18 日０時０分０秒～31 日０時のログファイルを使用した。

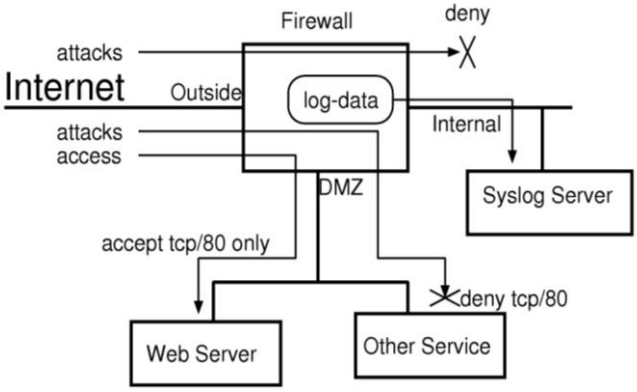

図２.実験環境

4.　データの解析

4．1　頻度分布からの DoS 攻撃の検出

まず頻度分布から DoS 攻撃の検出を試みる。

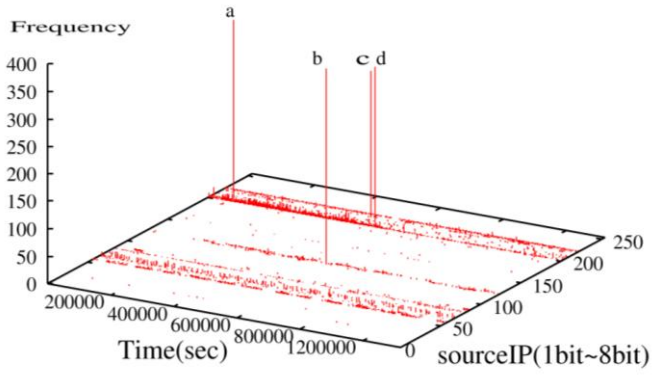

図３．IP アドレスの頻度分布

図３は x 軸が時間（sec）、y 軸は送信元ＩＰアドレスの上位８ビットにより集約した IP アドレス空間、および z 軸は該当する送信元 IP アドレスを持つパケットの頻度を表している。頻度が大幅に増加しているポイントは、ａ、ｂ、ｃ、ｄの点である。その４つの部分の送信元ＩＰアドレスを特定するため、データからそれぞれの下位のアドレスごとに順に抽出した。

分析の結果、ａ，ｂ，ｃ，ｄともにそれぞれ同じ送信元ＩＰアドレスから１～３秒の間アクセスが集中しておりアドレスが分散していない、したがって

DDoS 攻撃ではなく特定のホストからの DoS 攻撃と考えられる。また、[2]からドメインから国を割り出し表示したのが表１である。

表１． 上位４サイトのドメインの情報

	sourceIP	頻度	ドメイン	国名
a	202.142.88.36	290	IN	India
b	122.124.129.230	355	TW	Taiwan
c	202.248.97.74	202	JP	Japan
d	217.159.171.203	217	EE	Estonia

４．２ エントロピー

複数のホストからの分散したアクセスを検出するため、より詳細な IP の情報に基づき分析するため、送信元 IP アドレスの上位 16 ビットを抽出し、エントロピーの時系列変化を求めた。ここで、window サイズは 1200 秒(30 分)、および 3600 秒(60 分)にした場合のエントロピーの時系列の変化をそれぞれ図４、および図５に示す。スライド幅はともに 300 秒である。

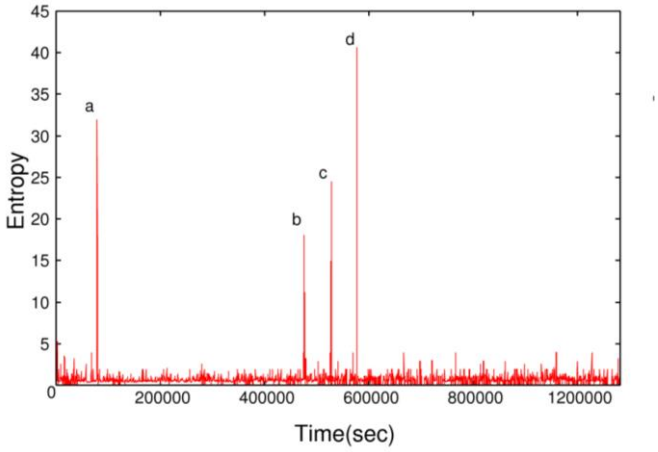

図４． window サイズ 1200 秒の場合の
エントロピーの時系列変化

図４と図５を比較した場合、図４のａ，ｂ，ｃ，ｄは各々ｘ軸の経過時間から図５の４点に対応していることがわかった。window サイズが 1200 秒において、頻度情報で検出した４点以外、エントロピーは微変動しかしておらず、頻度情報で得ることができなかったアクセスを検出することはできなかった。

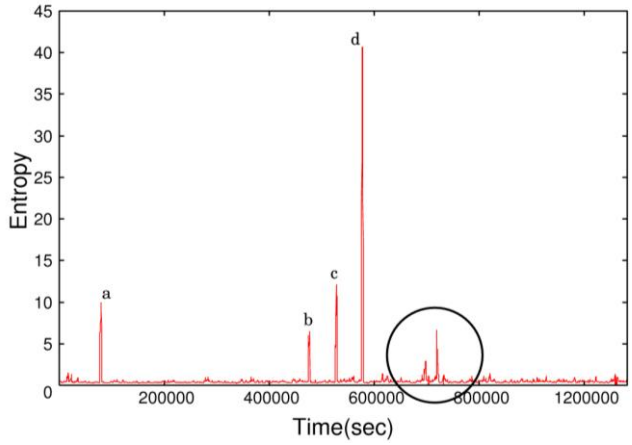

図５． window サイズ 3600 秒の場合の
エントロピーの時系列変化

図５においては、window サイズを３倍にした場合のエントロピーの時系列変化を示す。同じようにａ，ｂ，ｃ，ｄの４箇所は変化しているのみならず、円で囲んだ部分にエントロピーの特徴が確認できた。詳細に解析した結果、この時間帯に異なった複数の送信元 IP アドレスから少ない件数のアクセスが確認できた。しかし、これらの頻度の件数から DDoS 攻撃ではないと考えられる。複数の送信元 IP アドレスから一斉に不正アクセスが行われた場合検出できることが証明できたので同じように DDoS 攻撃も検出できるはずである。また、window サイズ大きさに依存して検出できる場合とできない場合があることがわかる。

５．おわりに

本研究ではアクセス頻度だけでは検出困難な送信元 IP アドレスが分散している DDoS 攻撃が行われた場合でもエントロピーを使用することで検出できることが可能であることが実証できた。また window サイズによって検出できる場合とできない場合があるので、実装する際にはそのＦＷのアクセス頻度のパターンに合わせて適正な window をチューニングする必要がある。またエントロピーを求めるとき window サイズ、スライド幅によって処理時間が大きく変わってくる。特にスライド幅を秒単位細かく設定したとしても、今回の解析ではグラフのｘ軸が細かくなるだけで解析するうえであまり効果が得られなかった。またスライドさせる度にエントロピーを計算する回数が増加するので値を小さく設定すると処理時間が長くなる。

今回の解析に使用したログデータ中には残念ながら DDoS 攻撃は含まれていなかったので、今後の研究では DDoS 攻撃を含んだデータで解析する必要がある。また、今回は 80/TCP ポートの deny 情報のみに注目して解析をしてきたが、他の ICMP および DNS などのプロトコルについても解析していきたい。

謝辞

本研究のデータ取得にあたり、FW ログの提供をご快諾いただいた八代工業高等専門学校情報処理センター長池田直光准教授、ならびにログ取得について技術面でご協力いただいた情報処理センタースタッフの方々に心からの感謝の念を表して謝辞とさせていただきます。

参考文献

[1] L.Feinstein, D.Schnackenderg, R.Balupari, D.Kindred, ”Statistical Approaches to DDoS Attak Detection and Response”, Proceeding of the DARPA Information Survivability Conference and Exposition (DISCEX’03)

[2] IANA ,Internet Assigned Numbers Authority, URL http:www.iana.org

問い合わせ先：中嶋 卓雄
〒 862-8652 熊本市渡鹿 9-1-1、九州東海大学
工学部 情報システム学科
Tel:096-386-2837
E-mail：taku@ktmail.ktokai-u.ac.jp