3T-3

パケット解析による DoS 攻撃の検知と識別

筆谷　光雄†　　西村　俊和‡　　小川　均‡

立命館大学大学院理工学研究科†

立命館大学情報理工学部情報コミュニケーション学科‡

1. はじめに

近年，インターネットの普及，ネットワークサービスの増加に伴い，コンピュータウィルスや DoS(Denial of Services)攻撃によって引き起こされるネットワーク障害の増加が考えられる．これらの障害に対して，IDS(Intrusion Detection System)やファイアウォールといったセキュリティ技術が利用されている．しかし，これらの運用にはある程度のスキルと経験が必要であり，障害の原因を追究するといった作業には多大なコストと労力を要し，管理者の負担がますます大きくなってしまう．さらに，日々新たな不正アクセス手法やウィルスが開発され，既存の技術だけでは防ぐことができなくなってきている．

ネットワーク障害には大別すると二種類の要因が考えられる．ひとつは電源が落ちているといった物理的な要因である．もう一方は，ウィルスや(D)DoS 攻撃によるもので，その中でも，大量の不要パケットによる帯域枯渇やセキュリティホールをつき不正処理を起こさせるような不正パケットが原因となることが多くなっている．[1]

そこで，パケットを多角的に解析し，障害を引き起こす理論的根拠を配慮した自動検知手法について考察を行なうことで，早期に DoS 攻撃の有無を検知し，障害の原因を追求できるシステムを提案する．

2. 提案システムの概要

本システムに必要な機能を以下にあげる．

- パケットダンプ解析機能
- 攻撃検知機能
- 攻撃識別機能

管理者の負担をできるだけ軽減する，攻撃を早期に検知，識別するために全ての機能を自動化し，処理を行なう．

パケットダンプ解析機能では流れてくるパケットを単位時間ごとにモニタリングし，そのログファイルをリアルタイムで解析する．

次に解析結果を攻撃検知機能に通知し，攻撃の有無を判断する．

最後に，未知攻撃を含めた攻撃を識別するために，解析結果を基に推論を行ない，攻撃の特定もしくは攻撃の類似性を導き出す．

本システムの構成例を図 1 に示す．

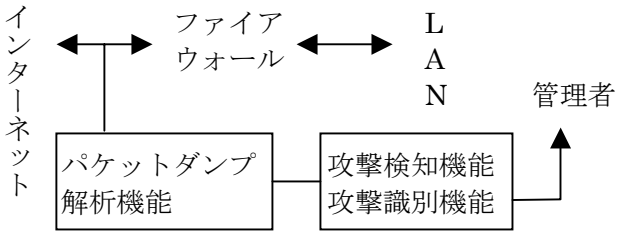

図 1　構成図

2.1 攻撃検知手法

攻撃の有無を判断するためにパケット解析データを用いる．単位時間に流れるパケット総数，各 TCP フラグ数，送信元，送信先 IP アドレス，送信元，送信先ポート番号，パケットサイズなどを多角的に解析した情報とそれらの相関分析によって得られる情報を用いる．

相関分析とは 2 変数間(x,y)の関係の度合いを数値的に分析する方法である．計算によって求められる相関係数 r は-1 から+1 の間の値をとる．相関関係がある場合，直線上に分布するが，異常があった場合に図 2 のようにずれが生じ，異常だと判断できる．ここで縦軸は Syn フラグ数，横軸は Ack フラグ数を示している．

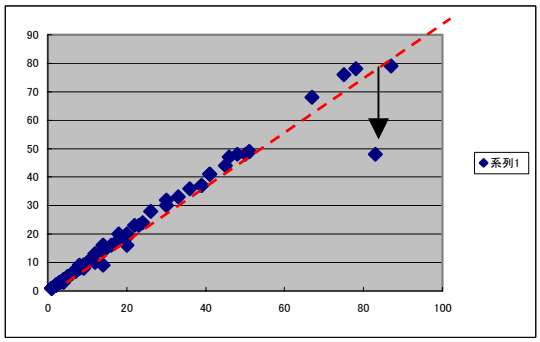

図 2　相関分析結果

「Detection and identification of DoS attacks by packet analysis」

†「Mitsuo Fudetani・Ritsumeikan University」

‡「Toshikazu Nishimura・Ritsumeikan University」

‡「Hitoshi Ogawa・Ritsumeikan University」

2.2 攻撃の分類

攻撃と判断された場合，その攻撃を識別するアプローチを以下の 3 種類に分類する．

１．パケット不均衡

通常，通信を行なう際には決まったパケットの流れが存在する．例えば，TCP 通信の際に必ず行なわれるスリーウェイハンドシェイクがある．クライアント（A）は対象サーバ（B）に対して Syn パケットを送信する．次に B は A に Syn と Ack のパケットを返信し，最後に A は B に Ack パケットを送信する．ここでは単位時間当たり Syn 数≒Syn+Ack 数≒Ack 数が成り立ち，もしその数に不均衡が生じた場合，異常があったと考えられる．この不均衡から DoS 攻撃を識別する．[2]

２．大量の不要パケット

Ping Flood，UDP　Flood，OpenTears のように通信を目的としない大量の不要なパケットによって帯域を枯渇させる DoS 攻撃を識別する．

３．規定外のパケット

Ping of Death，Land Attack，Smurf のように通常では起こりえないパケットを送り，ターゲットをクラッシさせる DoS 攻撃を識別する．

2.3 学習を用いた識別手法

実際に DoS 攻撃が行なわれた事例から，その特徴を学習することでルールを獲得し，同種の攻撃を発見する．学習には説明に基づく学習（EBL：Explanation Based Learning）を用いる．これは領域知識を用いることで目標概念を満足させ，一般化の証明を行なっていく学習手法である．[3]

ここで目標概念を与える．あるアドレス IPA に異常があれば攻撃だと判断するというルールを以下のように表す．

```
IF      Unusual(IPA)
THEN    ThereExistAttacks
```

ルール獲得の手順を Syn Flood を用いて説明する．Syn Flood はスリーウェイハンドシェイクの最後に送られる Ack が返ってこないことで SYN_RECEIVED 状態となり，正常なアクセスを受け付けられなるという障害が発生する．これは訓練例として次のように与えられる．

P1=Packet(192. 168. 0. 8, 172. 24. 3. 2, Syn).
P2=Packet(172. 24. 3. 2, 192. 168. 0. 8, Syn+Ack).
P3=Packet(192. 168. 0. 8, 172. 24. 3. 2, Ack).
Num(P1)=2000.
Num(P2)=2000.
Num(P3)=0.
Num(P2)-Num(P3)=2000.

ここで Packet(A,B,C)は A（送信元 IP アドレス）から B(送信先 IP アドレス)へ C(TCP 制御フラグ)を送ることを表し，同じ組み合わせを 1 つと考える．Num(P)は P の 10 秒間の合計を表す．

次に領域知識を次のように表すことができる．

```
R1  IF   Imbarance(Packet(IP2,IP1,FLAG2),
                   Packet(IP2,IP1,FLAG3))
    THEN Unusual(IP1)
R2  IF   P2 = Packet(IP2, IP1, FLAG2),
         P3 = Packet(IP1, IP2, FLAG3),
         Replay(Packet(IP2,IP1,FLAG2),
                Packet(IP1, IP2, FLAG3)),
         Num(P2) – Num(P3) = N,
         N > 1500
    THEN Imbalance(P2, P3)
R3  Replay(Packet(IP1,IP2,Syn),
           Packet(IP2, IP1, Syn+Ack))
R4  Replay(Packet(IP2,IP1, Syn+Ack),
           Packet(IP1, IP2, Ack))
```

ここで Replay(A,B)はパケット A の後にはパケット B が流れることを示す．

EBL より次の新しいルールが導出できる．

```
IF      P2 = Packet(IP2, IP1, FLAG2),
        P3 = Packet(IP1, IP2, FLAG3),
        Reply(Packet(IP2,IP1,FLAG2),
              Packet(IP1, IP2, FLAG3)),
        Num(P2) – Num(P3) = N,
        N > 1500
THEN    ThereExistAttacks
```

本手法で得られたルールは，Syn Flood だけでなく，同様のスリーウェイハンドシェイクを利用した攻撃も認識できる可能性がある．(ただし，制御フラグの定義があらかじめ領域知識に必要)．これにより管理者の負担の軽減や，早期検知が実現でき，さらに将来的に起こりうる攻撃にも対応できる識別システムが構築できると考えられる．

3. まとめ

本稿では Syn Flood を例に EBL を用いた識別手法を提案した．今後，DoS 攻撃の事例を集め，パターンの学習を行ない，提案手法の有用性を考察していきたいと考えている．

参考文献

[1] Joel Scambray 他:”クラッキング防衛大全 windows2000 編”, 翔泳社(2003)

[2] 海崎良:”ネットワーク運用における DoS 攻撃に関する研究”, 慶應義塾大学政策メディア研究科(2002)

[3] 前田隆, 青木文夫: “新しい人工知能 発展編”, オーム社(2000)