攻撃モデルを用いたDDoS攻撃の予兆検知方式

三友 仁史、滝澤 文恵、久保田 和己、鳥居 悟、小谷野 修
富士通株式会社

1. はじめに

DDoS 攻撃による実被害を回避するためには将来起こりうる DDoS 攻撃を予知する必要があるが、従来はセキュリティシステム管理者によるログ解析による方法が中心であり、管理者に大きな負担を強いてきた。そこで我々は、DDoS 攻撃を自動的に予知することを目指した攻撃予知機構に関する研究を行ってきた[1]。

本稿では、DDoS 攻撃予知の為の第一ステップとして、ネットワークトラフィックから DDoS 攻撃の予兆を検出する方式について提案する。なお、DDoS 攻撃を予知した後、実際にそれを回避する方式については、[2][3]を参照されたい。

2. DDoS 攻撃予知機構

ここでは DDoS 攻撃予知機構について説明する。

2.1. システム概要

以下に DDoS 攻撃予知機構の概要を示す。我々はこの機構を、ネットワーク(ISP、イントラネット等)毎に一つずつ設置することを想定している。

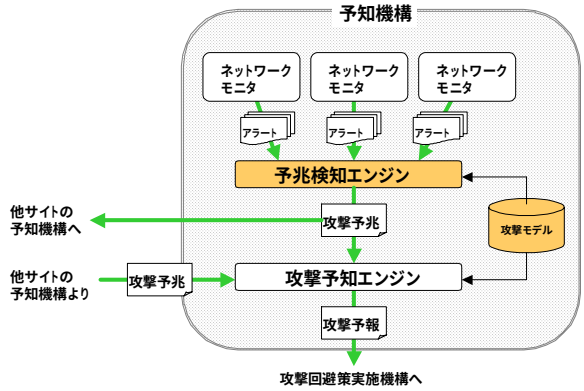

図１：DDoS 攻撃予知機構の概要

2.2. 予知機構実現への基本的考え方

ここでは DDoS 攻撃予知機構実現への基本的考え方について簡単に説明する。攻撃者が DDoS 攻撃を発生させるためには、DDoS エージェントを複数の踏み台ホストに仕込み、最終的にそれらに大量のトラフィックを生成させるといった準備行為が必要である。ここで、DDoS エージェントとは、DDoS を引き起こす大量のトラフィックを生成するネットワークツールである。

準備行為は一般にネットワークを介して行われる為、これらはネットワークモニタにより検出することが出来る。我々は、この準備行為を DDoS 攻撃の予兆と定義する。さらに、この予兆を広範から収集して関連付けることにより、将来起こり得る DDoS 攻撃の予知を実現出来ると考えている。

本稿で主に、このうち DDoS 攻撃の予兆を検出する方式について述べる。なお、図中の攻撃予知エンジンについては、本稿で詳細は述べない。

2.3. 攻撃予兆の検出

予兆の検出には２つの要素技術が必要である。

- 攻撃モデル
  準備行為の手順を表したモデル
- 予兆検出エンジン
  アラートに攻撃モデルをリアルタイムに適用し、攻撃予兆を検出・出力するエンジン

攻撃者による「一連の手順」を構成するアラートそれぞれの検出は既存ツール(ここでのネットワークモニタ)でも可能であるが、そのままでは大量の誤報が避けられない。そこで、イベントそれぞれを関連付けて手順として検出するアプローチを採用した。これにより、誤報を抑えながら、DDoS 攻撃の予兆を検出することが可能となる。

3. 攻撃モデル

攻撃モデルは、以下のようなアラートの状態遷移図で表すことが出来る。

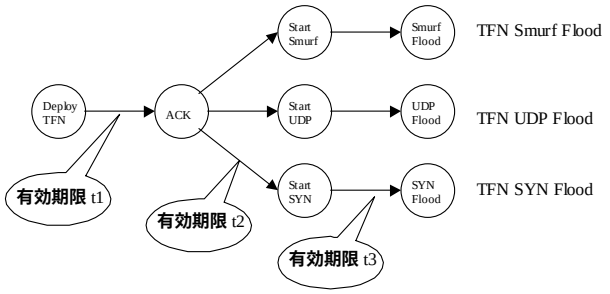

図２：攻撃モデル

ここで、各アラート間に遷移の有効期限を付与している。このモデルにより、DDoS 発生までの攻撃者の侵入の手順を記述することが出来る。

なお、攻撃モデルのインスタンスは、机上の調査に加えデータマイニングにより作成する予定

Method for detecting omen of DDoS with attack models
Masashi Mitomo, Fumie Takizawa, Kazumi Kubota, Satoru Torii, Osamu Koyano,
FUJITSU Limited

である。本稿で詳細は述べない。

4. 予兆検知エンジン

予兆検知エンジンは、ネットワークモニタによるアラートに攻撃モデルをマッチングし、攻撃予兆を検出するコンポーネントである。攻撃予兆は、検出した攻撃モデルのＩＤと、その攻撃元／先等からなる情報である。

本エンジンは内部で、監視対象ホストそれぞれの通信の「状態」を保持している。これは、当該通信で進行している攻撃モデルと、その進捗度（状態遷移が何番目まで進んだか）の組で表される。これにより、予兆検知エンジンは攻撃モデルのマッチングを行うことが可能となる。

5. 基本性能の評価

ここでは、攻撃予知機構の実用化に向けた検討のベースとする為、攻撃予兆検知方式の基本性能を評価した結果について述べる。

5.1. 評価方針

攻撃予兆検知方式に要求されるのは処理のリアルタイム性である。ここで、処理速度に影響を与える主なパラメータは、保持する状態及び攻撃モデルの数であると考えられる。

以下ではまず、本予兆検知方式の想定利用環境における、これらパラメータの規模を机上評価する。次に、当該規模のパラメータを実現できる入力データを用意し、試作した予兆検知エンジンの処理速度を測定・評価する。

5.2. パラメータ規模の評価

１） 状態

エンジンが保持する必要がある状態数は、ある実運用環境におけるアラートログから求めた。このログは、18 個のクラスＢまたはＣのネットワークを 12 週間監視して得られたものであり、約 246 万のアラートが含まれている[1]。このことから、一つのネットワークを監視対象とすれば、最悪の場合でも 246 万／18 ＝ 14 万の状態を保持すれば十分であると考えられる。

２） 攻撃モデル

必要な攻撃モデルの数は、既知の DDoS ツールの種類(SANS のレポート[4]では十数種が紹介されている)、及びその攻撃のバリエーション(UDP FLOOD、SYN FLOOD、SMURF 等)を勘案して、当面は１００個程度あれば十分と見積もられる。

5.3. エンジンの処理速度

エンジンの核である、攻撃モデルマッチング機能のみを実装し、それに実験環境のログを適用して処理速度を測定した。

まず、実装の前に、エンジンのメモリ使用量を予め見積もった。これは、もしそのサイズがメモリ展開できないほど大きな場合、メモリ管理の機構を組み込む必要が生じるためである。

表１：必要メモリサイズ

	必要数 (a)	1つ当たりのサイズ(b)	必要サイズ (a × b)
攻撃モデル	100	500B	50KB
状態	140000	100B	14MB

ここで、それぞれの 1 つ当たりのサイズは、予兆検知エンジンで採用するフォーマットを元に見積もった。結局、必要サイズの合計は 14 メガバイト程度でありこれは十分にメモリ展開できるサイズであることが判明した。

実験環境(Turbolinux WS 7.0、Celeron 500MHz、RAM 256MB)において、想定される運用環境でのパラメータ規模で予兆検知エンジンの処理速度を測定したところ、およそ 3000 アラート／秒であった。これは、前記アラートログから算出した「単一ネットワークのアラート発生速度」約 0.02 アラート／秒の 150000 倍である。従って、クラスＢ／Ｃのネットワークであれば、本方式により遅延無く攻撃の予兆を検出できることが示された。

6. まとめ

本稿では、DDoS 攻撃の予兆を検出する方式について述べ、その基本性能について評価した。その結果、本方式によると、処理速度及び消費メモリが共に、実用化を想定した際の許容範囲に収まることが示された。

今後は、まず攻撃予兆から DDoS 攻撃を予知するフェイズの方式について検討し、「DDoS 攻撃予知機構」の全体像を明らかにする。さらに、実証実験を通じて、当該機構の有効性を実証する予定である。

謝辞

本研究は、通信・放送機構の委託研究テーマ「サービス不能化（DDoS）攻撃に対する防御技術に関する研究開発」の一環として行われているものである。

参考文献

[1] 久保田 他, “*不正アクセスシナリオの導出に向けた検知ログ解析*”, 情報処理学会 第 64 回全国大会, Mar. 2002

[2] 羽生 他, “*DDoS 攻撃回避機構の試作*”, 情報処理学会 第 65 回全国大会, Mar. 2003

[3] 森田 他, “*DDoS 攻撃回避を目指した組織間連携方式*”, 情報処理学会 第 65 回全国大会, Mar. 2003

[4] http://www.sans.org/rr/firewall/prevention.php