不正アクセスパケットのシャボン玉による可視化

研究指導　菊池浩明　教授

東海大学　電子情報学部　情報メディア学科

4adm1120 松谷　亜紀

目次

第1章　はじめに

近年、ブログやSNSの誕生によってネットワーク利用者が急増し、日常生活に「IT」という言葉が浸透しつつある。一般の人でもコンテンツの利用のためにネットワークに滞在する時間が以前よりも増えた。しかし、ウィルスや不正アクセスといった脅威ははいまだ解消されていない。それを代表とされる事例として、マスメール型ウィルスが流行しつつあることが挙げられる。一時期LOVELETTERに代表されるメールの添付ファイルを実行することで感染してしまうウィルスが大流行したことがあったが、一般の人の利用の増加によって、近年また感染数が比例して増加している。また、企業においてもウィルス感染被害が急増しておりそれが引き起こす問題によって企業価値の低下や信頼の損失が生じている。

このように、神出鬼没な攻撃者に順次対応するのは困難であり、対応しきれないのが現状である。そこで、これらの攻撃の傾向や変化を検出し，対策に生かせるようにする必要がある。

第2章　不正アクセスパケット

2.1　不正アクセスパケット

ネットワークを経由し、他のコンピュータに許可なくアクセスすることを不正アクセスとし、そのパケットを不正アクセスパケットという。

本研究では不正にポートスキャン等を行う不正アクセスのパケットを用いる。

2.2　ログデータ

可視化を行うパケットのデータはセンサにて観測されたログデータを用いた。
センサとはネットワーク上でパケットを観測するホストであり、届いたパケットに対して応答は行わない為、本研究では届いたパケットを不正アクセスパケットと仮定した。
ログデータから読み取れる情報は、不正アクセスパケットの到着した到着日付、到着時間、標準時間、宛先 IP アドレス、プロトコル、送信元 IP アドレス、センサ番号、宛先ポートであり、これらはセンサに不正アクセスが行われる毎に一行作成される。

センサによってばらつきがあるが、この不正アクセスログデータは一日で数行から数万行並び、これらを手作業で見、特徴を把握するには以下の 2 点の問題が挙げられる。
(1)膨大なログデータを見ていく難解さ
(2)文字の羅列である為、細かな特徴点を見落としやすい
そこで、本研究では送信元情報と宛先情報（IP アドレス，ポート番号）に注目し、特定の送信元 IP アドレスが複数の宛先 IP アドレスにパケットを走査する様子を、可視化することによって、その特徴を読み取り易くすることを目的とする。

2.3　センサの届いた場合の IP

なお、可視化にあたり、センサは IP に変換した。以下にそれを記す。

sensor01	208.162.126.223
sensor02	206.79.184.165
sensor03	205.9.171.232
sensor04	196.120.215.172
sensor05	134.144.94.10
sensor06	158.246.212.111
sensor07	204.233.24.48
sensor08	206.167.141.20
sensor09	204.191.149.194
sensor10	75.64.57.33
sensor11	75.64.57.33
sensor12	129.75.255.203
sensor13	196.100.168.219
sensor14	207.20.33.124
sensor15	126.161.195.49
sensor16	77.247.248.254
sensor17	190.102.151.187
sensor18	197.115.22.98
sensor19	72.1.35.208
sensor20	206.158.130.90
sensor21	193.149.140.28
sensor22	74.179.147.20
sensor23	190.87.223.15
sensor24	191.188.255.205
sensor25	193.32.158.244
sensor26	207.102.209.227
sensor27	207.56.91.102
sensor28	129.105.127.113
sensor29	130.133.228.130
sensor30	75.224.84.87

第3章　可視化の方式

3.1　可視化軸

本研究では可視化の表現方法として、箱形の空間を用いた。

図 1 において、右側のメッシュが送信元，左側のメッシュが宛先を表す．可視化軸は，縦軸が IP の第 1 オクテット(32bit の上位 8bit,max=255),奥行きがポート番号(max=65535)を表す.

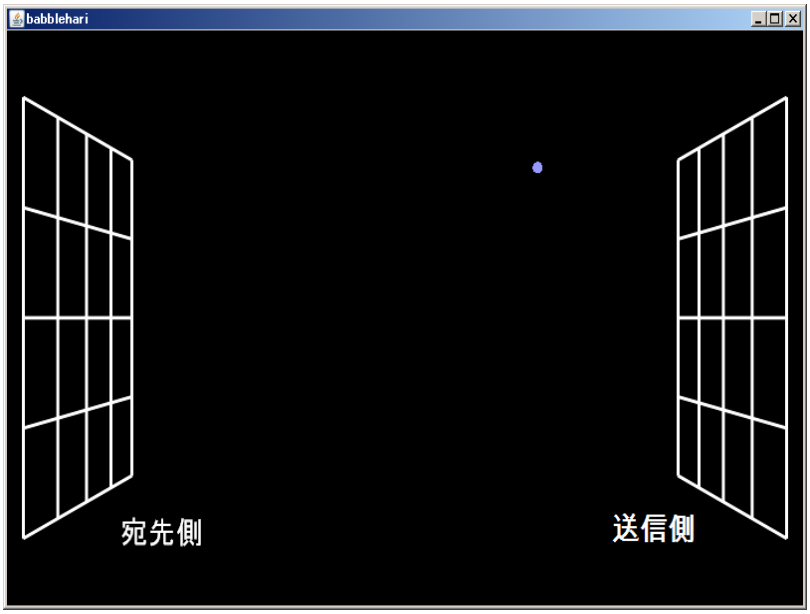

図 1　可視化軸

3.2　アニメーション

今回の可視化では不正アクセスをシャボン玉に見立ててアニメーション可視化を行った。

1 つのシャボン玉を右側から左側に移動させることによって、1 つのパケットを観測したことを表す。パケットの飛ぶ順はセンサで観測された日付時間順に等間隔で 1 つずつアニメーションを行い、同時に飛んできた場合はログデータに蓄積された順に飛ぶ。

また TCP や UDP といったプロトコルとの判別のために ICMP パケットはポート番号の原点を通る。

3.3　実装

本研究では JAVA3D により可視化を行い、アプレットで実装を行った。

手順は以下の通りである。

1. ログデータから送信元の IP アドレスのオクテット，ポート番号、宛先センサ番号、ポートを取り出す
2. センサ番号から憶測される IP アドレスの１オクテットに変換
3. Java3D の alpha によってアニメーションのタイミングをスケジューリング
4. Interpolator によってアニメーションとして実装

また、固定の角度からパケットの動向をみるのでは、ポート番号等の情報を読み取り難いことがある。そこで java3D の MouseBehavior 機能を利用し、追加することによって操作者がマウス操作によって可視空間全体を回転させるようにし、任意の角度からパケットの動向がみられるようにした。実行画面を図 2 に記す。

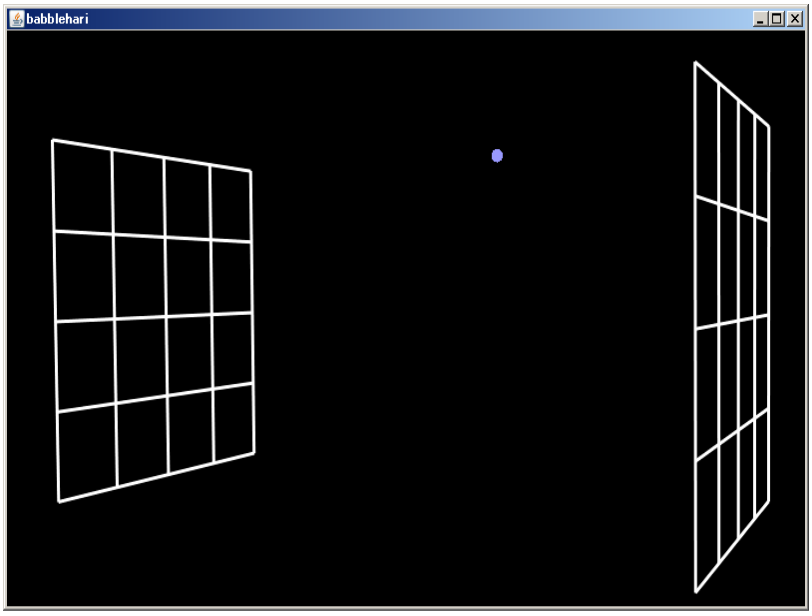

図 2 回転機能の追加

第4章　可視化提案

今回の研究では完成には至らなかったが、以下に当初の目標であった可視化を提案として記す。

4.1　Java3D とは

可視化提案をする前に本研究で用いた Java3D について特筆させていただきたい。

本研究で用いた Java3D とはサン・マイクロシステム社から提供された、Java Media API の一部である 3D グラフィックスアプリケーションを作成するためのプログラミングインターフェイスである。設計思想は VRML に大きく影響を受け、他の低レベルの API の長所が組み合わせられており、非常に効率的にバーチャルワールドを創造することができる。

レンダリングするためには描画空間に関する全ての情報を設定しておくシーングラフをと呼ばれるものの中に予め描画したいジオメトリーのデータとその属性、物体の動き、回転や拡大縮小といった視点の動きの情報を指定しておくことによって描画をすることができる。

4.2　到着時間の考慮

今回の可視化では等間隔でのアニメーションにより、到着時間を考慮したものにまでは至らなかった。短時間に集中的に不正アクセスが行われた場合も長時間にわたって攻撃した場合も同じ間隔であるため、時間の特徴を見ることができない。

そこで、解決する可視化法として、全体の時間の尺度からタイミングを割り出し、そのタイミングとアクセスパケット到着日時間をかけることで到着時間を考慮する方法が挙げられる。

4.3　同時時間パケットの考慮

前章でも触れた通り、不正アクセスパケットが同時時間に飛んでくることがある。今回はログデータに記載された順にパケットを飛ばしたが、これでは実際に到着した感覚とずれが生じてします。

それを解決可視化として同時時間にセンサに不正アクセスパケットが複数到着した場合、その複数のしゃぼん玉が宛先側メッシュに到着する可視化が挙げられる。

4.4　JAVA3D での実装

上記の 2 点を JAVA3D で実装する場合、問題となってくるのはタイミングである。

Java3D は基本的に alpha によってタイミングを指定すれば等間隔に自動的にアニメーションを行うリテインドモードで作成されることが多く、複雑なタイミングの調整は難しい。

それを設定するモードとしてイミディエートモードが挙げられる。しかしながら、イミディエートモード問題点は、描画の詳細なタイミングの制御ができる代わり、描画に至るまでのすべてを制御しなければ描画されない点である。

第5章　結論と今後の課題

5.1　結論

「ボット」などの影響により、複数の送信元から同時に送られる不正アクセスパケットや、特定ホストの複数ポートへの不正アクセスパケットが飛ぶ様子を視覚的に捉えることができた。

5.2　今後の課題

今回の可視化では、不正アクセスパケットが発信され到着する様子を可視化した。しかし、到着時間と同時時間パケットを考慮したプログラムまでには至らなかった。

今後の課題として、同時刻・金時刻に宛先側に到着したパケットが複数ある場合に複数のシャボン玉が飛ぶプログラムにし、実時間に沿ってパケットを可視できるようにすることが挙げられる。

参考文献

[1]中尾ほか,「インシデント分析センタ nicter の可視化技術」, 情報処理学会, CSEC2006 pp. 313-3182006.

[2]石黒ほか,「インターネット上の不正パケットの送信元 IP アドレスの分布に関する分析」, 情報処理学会, CSS2006, pp. 507-512, 2006.

[3]林ほか,「java3D による 3 次元 CG プログラミング」, コロナ社.

[4]Henry Sowizral ほか,「The Java 3D API 仕様」, ASCII 社.

謝辞

本研究にあたって、暖かいご指導を受け賜りました東海大学電子情報学部情報メディア学科菊池浩明教授に心から感謝申し上げます。

また同時に多大なご指導と助言を受け賜りました小堀氏、畠山氏に深くお礼申し上げます。