4Y-7

大規模ネットワークログデータの可視化を利用した ネットワーク管理の支援に関する研究

山根 寿† 土井 章男†
岩手県立大学 ソフトウェア情報学部†

1．はじめに

インターネットの世界において、不正アクセスは大きな問題になっている。この問題を未然に防ぐ、もしくは素早く対応するためには、ネットワーク管理者によるネットワークログ調査が考えられるが、検知システムから発せられた警告箇所のログ調査は多大な時間と労力を必要とする。そこで本研究では、時系列ネットワークログデータからの障害箇所の発見とトラフィック状況の可視化により、ネットワーク管理の支援を行う手法を提案する。

2．提案手法

一般に数万行あるネットワークログデータを直接閲覧する事は非効率的であり、可視化の要望が大きい。しかし既存の可視化ツールである、Site Manager[1]や Cone Tree[2]をログデータの可視化に直接使用できない。

そこで我々は、図 1 の情報を持つログデータを対象にネットワークログデータの可視化を行う。ネットワーク内部の IP アドレスと外部の IP アドレス各々を配置する 2 つの xy 平面を用意する。IP アドレスの通信は、両 IP アドレス間を直線で連結して表現する。また、(1)Smurf と DDos では複数の端末から 1 つの端末に集中して通信が起きる、(2)他端末からのポートスキャンでは 1 対 1 の通信が繰り返し起こる[3]という観点から「アクセス数」を重要視し、透明度や着色による強調表示を行う（図 2)。

日付	時間	受信IPアドレス	送信IPアドレス	データ量	プロトコル
18Jul2003	0:00:01	172.18.2.129	900.182.169.36	152	ntp
18Jul2003	0:00:03	172.19.4.112	900.181.141.76	786	http
18Jul2003	0:00:03	172.19.4.112	901.209.169.202	767	http
18Jul2003	0:00:03	172.19.4.112	902.44.238.249	1565	http
：					

図 1：ネットワークログデータ

A study of network management support using visualization of large-scale network log-data
Hisashi Yamane† and Akio Doi†, Iwate Prefectural University, Faculty of Software and Information Science†

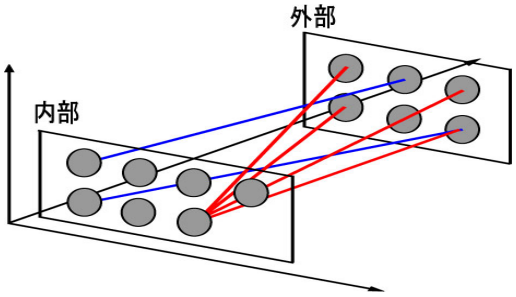

図 2：可視化手法

3．実装

実装は Windows 2000、XP 上にて Visual C++、MFC 及び OpenGL を用いて行った。

受信側端末の画面空間への配置方法は、第 2 オクテッドレベル毎にまとめた事により、直感的に理解できる。また、オブジェクトの密集による見づらさを防ぐために「画面空間の拡大を防ぎつつオブジェクト間の隙間は残す」という点を考慮した。xy 方向への第 2 オクテッドレベルにおける縦方向の配置数 h は

$$h = discard(\sqrt{n}) \quad (1)$$

横方向の配置数 w は

$$w = raise(\sqrt{n/h}) \quad (2)$$

ここでの $raise(a)$ は小数点を切り上げる関数、$discard(a)$ は小数点以下を切り捨てる関数、n は全体の個数である。

式(1)、(2)により、xy 方向への配置数を決定し、第 2 オクテッドレベルの配置は縦横それぞれの方向の最大枠に揃えて配置した。

図 3 に 4 つの第 2 オクテッドレベルの配置例を示す。

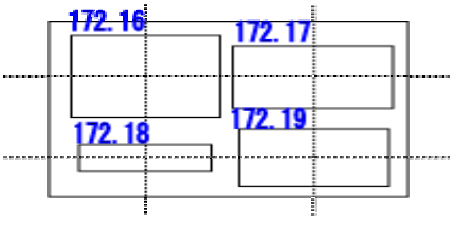

図 3：端末配置方法

4．評価

評価には、2003 年 7 月 18 日に岩手県立大学のネットワークで取得された 1 日分のログデータを用いた。図 4 に 1000 回のアクセスを記録したネットワークログデータへの適用結果を示す。

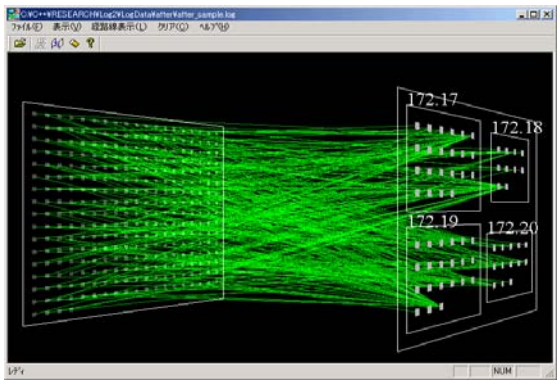

図 4：ログデータの表示例

単純に適用すると、アクセスを表す経路線が重なり合ってしまい、全体像の把握が困難である。そのため、最も多くのアクセスがあった端末に対する経路線の透明度αを不透明として表示した（図 5）。透明度αは、式(3)により決定する。

$$\alpha = i / \max \qquad (3)$$

ここでiは同じ IP の出現した回数、max は最も多い IP の回数である。

この結果、経路線の重なりを防ぐと共に 172.18 に属する端末にアクセスが集中している事が分かる。

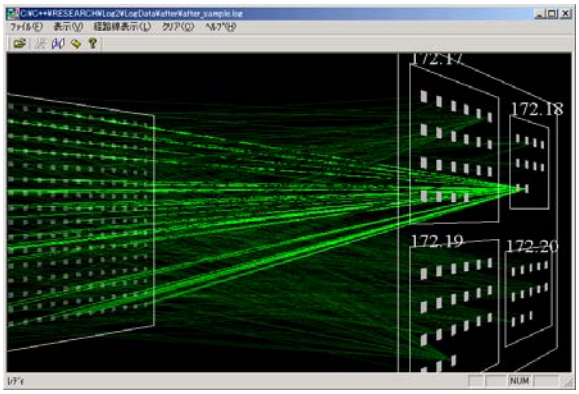

図 5：透明度を考慮した表示例

端末を配置した 2 つの平面間の Z 軸を時間軸に見立て、アクセスが起こった時間の経路線上にデータ量を色で区別した三角錐を配置した。これにより、連続してアクセスがあった場合の強調が可能となった（図 6）。

図 6：三角錐によるデータの表現

また、個別の IP アドレスに対するサポートとして、ポートへのアクセス状況を可視化した。図 7 では、横軸は時間、各三角形は各ポートへのアクセスを示す。

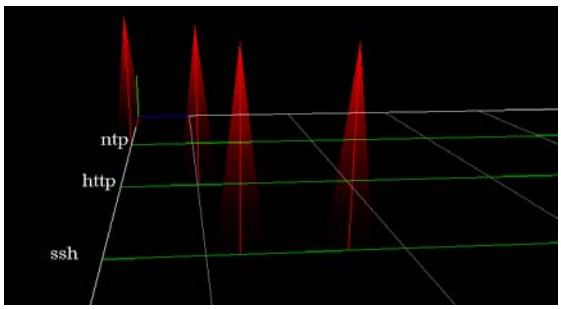

図 7：ポート情報の表示

5．おわりに

本研究では、大規模なネットワークログデータから不正アクセスの発見を支援する手法について提案し、実際のログデータに適用した。本手法により、集中的にアクセスを受けている部分の強調や、同 IP 間での連続的なアクセスの強調により、DDos や Smurf、ポートスキャン等の一定の性質を持った、ネットワーク上での攻撃の可能性がある通信を強調表示する事が可能となった。しかし、問題点として、今回表示したログデータよりも大規模なデータを扱う場合、経路線同士の重なりによる「埋没」が生じてしまう。その解決方法としては、ドットで区切られる IP アドレスのオクテッドレベルでの削減の他、任意にアクセス数の閾値を入力し、それ以下の経路線の表示を行わない事が考えられる。

参考文献

[1] SGI, Site Manager, http://www.sgi.com/

[2] XeroxPARC, ConeTree, http://www.parc.xerox.com/

[3] 寺田真敏・萱島信, 基礎から分かる TCP/IP セキュリティ実験, オーム社, H12.9.25