発信元偽装メール型ウィルスの感染源分析法

豊泉　洋*
* 会津大学 性能評価研究室
E-mail: toyo@u-aizu.ac.jp

観測サーバーで感染メールの到着間隔を観測することによって、ウィルスの感染源のサーバーから仮想的な距離を推定する分析技術を提案する。 発信元メールアドレスを偽装するコンピュータウィルス（ワーム）は、感染源の発見を困難にすることにより、感染拡大をはかる。このウィルスの感染源を特定するために、ウィルスの感染源がサーバーからどの程度離れた距離にいるかを推定する分析技術を提案し、その分析技術を実際のウィルスに適用した結果を示す。

Detect the Source of Worms with Spoofed Email Address

HIROSHI TOYOIZUMI*
*University of Aizu, Performance Evaluation lab.
E-mail: toyo@u-aizu.ac.jp

There are computer viruses or worms spreading by spoofing their email addresses. In this paper, we propose a novel method to estimate the distance from the machine infected with a worm to the server who received the infected Email, by just observing the inter-arrival time of infected emails.

1　はじめに

メールに添付される形で増殖するコンピュータウィルスやワームは、アンチウィルスソフトの導入や一般ユーザーへの啓蒙活動などの防御活動にもかかわらず増加の傾向にある。これらのワームの共通の特徴として、発信元アドレスの偽造があげられる。アンチウィルスソフトが受信したメールのワームによる汚染を検出しても、発信元が偽装されているため、感染の拡大を防ぐことができない。

こうしたメール型のウィルスのローカルなネットワーク内への感染を防ぐ効果的な方法の一つとして、ネットワークのゲートでのアンチウィルスによるメールの感染有無のチェックがある。しかし、ノート型のPC の持ち込みやファイルの交換などにより、ローカルなネットワーク内にも感染が広がる可能性がある。一旦、ローカルなネットワーク内に感染が拡大してしまうと、ゲートでのアンチウィルスによる防御では、感染の拡大を防ぎきれない。感染メールのヘッダや packet レベルの詳細な分析により、ネットワーク管理者は、これらの感染源を突き止めることも可能であるが、大量の感染メールが行き交う中で、詳細な分析で感染源を特定するのは、効率的でない。

コンピュータウィルス等の malicious mobile code のインターネット上での拡散を分析、防御する研究としては [1, 2, 3, 4, 5, 6] などがすでにあるが、いずれも感染源を偽装する形のワームの感染源の発見に対しては、有効ではない。

本論文では、発信元アドレスを偽装し、感染源の発見を困難にすることにより感染拡大をはかるコンピュータウィルス（ワーム）への対策として、感染メールの観測サーバーへの到着間隔や到着数を観測することによって、ウィルスの感染源がサーバーからどの程度離れた距離にいるかを推定する分析技術について述べる。この技術により、感染源が近い場所にいるときに、感染源からのウィルス除去等の対処が効率的に行える。

2　感染源と観測サーバーのネットワークモデル

ワームのネットワーク上での拡散とその観測の様子を次のようにモデル化する (図 1 参照)。

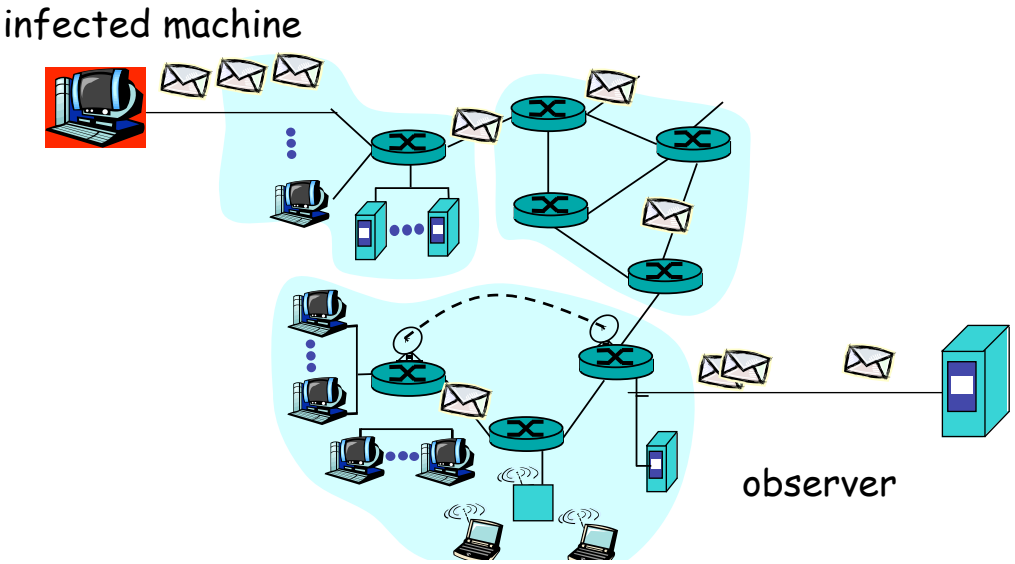

図 1: ワームの感染拡大と観測サーバー：感染源のマシンは一定間隔で感染メールを発信する。観測サーバーは、そのうちの特定のメールを観測する。

ネットワーク上の特定のマシンが何らかの原因で既知のワームに感染したと仮定する。また、ネットワーク上の特定の箇所には、観測サーバーがあり、この観測サーバーは、ワームの活動をモニターするために、既知のウィルスの最新の情報によりウィルスに感染したメールを検出する機能を持つとする。典型的には、観測サーバーはローカルネットワークのゲートに位置するメールサーバーに相当する。

ワームに感染したマシンは、次の感染先を見つけるためにマシン内にあるメールアドレスを検索し、発見されたアドレスから次の感染先を選択し、自分の複製を添付したメールを送付する。以下では、感染先は、宛先の選択はランダムであると仮定する。また、ワームはメールの送信元フィールドを詐称し、容易に発信元がわからないように偽装工作を行っているとする。感染源のマシンは、感染メールを一定間隔 d で次々に送信する。感染したメールは、宛先に向かってネットワーク上を転送されていく。

宛先がランダムに選ばれていると仮定したので、感染されたメールは、ネットワークの経路上の各ルーターで、ベルヌーイ試行によって経路が選択され、次のルーターへ転送されていく。特に、特定の感染メールが最終的に観測サーバーまで転送される確率を α とする。各ホップでの経路の選択確率が一定で β であり、感染源から観測サーバーまでのホップ数 m とすると、到達確率は $\alpha = \beta^m$ と表すことができる[2]。

サーバーで観測される n 番目の感染メールと $n+1$ 番目の感染メールのサーバーへの到着時刻の間隔（到着間隔）を X_n とする。すると上記のような仮定のもとで、到着間隔 X_n は次のように幾何分布で表すことができる。

$$P[X_n = dk] = (1-\alpha)^{k-1}\alpha. \tag{1}$$

したがって、平均 $E[X_n]$ および分散 $Var[X_n]$ は

$$E[X_n] = \frac{d}{\alpha}. \tag{2}$$

$$Var[X_n] = \frac{d^2(1-\alpha)}{\alpha^2}. \tag{3}$$

となる。

3 感染源までの仮想距離

感染メールの到着間隔のデータを統計処理し、感染メールの平均と分散が計算し、このデータから感染源までの仮想距離を推定する方法を考える。

観測サーバーは、感染源がネットワーク上でどこに位置しているかわからない上に、感染源がどの程度の頻度で感染メールを送信しているかわからないものとする。すなわち、感染メールの到達確率 α、および感染メールの送信間隔 d は観測サーバーに未知とする。この状態で、感染源までの距離を推定する。

さて、(2) と (3) より、感染メールがサーバーへ届く確率 α の推定値として

$$\alpha = 1 - \frac{Var[X_n]}{E^2[X_n]} \tag{4}$$

が得られる。さらに Section 2 のようなランダムモデルを仮定した場合、感染源から観測サーバーまでのホップ数が m とすると、到達確率は $\alpha = \beta^m$ となる。

[2]実際には、各ホップでの経路の選択確率は異なると予想されるが、本論文で導入する仮想距離では、同一であると仮定している。

(4) の両辺で log をとると、m は次の式で評価することができる。

$$m = \frac{\log \alpha}{\log \beta} = \frac{\log\left(1 - Var[X_n]/E^2[X_n]\right)}{\log \beta}.$$

以上の議論から、観測サーバーからみた感染源までの仮想的な距離を下記のように導入する。

Definition 1 (到着間隔観測による仮想距離). 観測サーバーからみた感染源までの仮想的な距離 m_β を次のように定義する。

$$m_\beta := \frac{\log\left(1 - Var[X_n]/E^2[X_n]\right)}{\log \beta}. \quad (5)$$

ここで、β は観測値から直接得ることは難しいが、適当なコンスタント (例えば 1/2) を仮定しても以下の議論には支障はない。

感染源までの仮想距離 m_β がどんな性質を持つかいくつかのケースを想定して、調べてみよう。

サーバーで観測される感染メールの到着間隔がほぼ一定となり、$Var[X_n] \approx 0$ となったと仮定する。この場合の感染源までの仮想距離は $m_\beta = 0$ となる。これは、感染源からのメールがすべて観測サーバーを通り、感染源となっているマシンが同一の local network の中にいる可能性が高いことを示している。

感染源から観測サーバーまでのホップ数が大きく、m が大きい場合には、幾何分布が指数分布に収束する。逆に、到着間隔が指数分布にしたがっている場合は、 $Var[X_n] \approx E^2[X_n]$ となり、$m_\beta = \infty$ となる。

多数の独立なソースからの感染メールの到着がある場合には、Poisson convergence より、到着過程は Poisson Process に弱収束し、到着間隔が指数分布となることが知られている [7]。したがって、m_β が大きい場合には、感染源が充分遠い場所にあるか、多数の独立な感染源からの感染メールであることが予想される。

結局、仮想距離 m_β が小さい場合には、それを観測したサーバーから近いところに感染したマシーンがいる可能性が高いことが推定される。

4 Counting Process による仮想距離

到着間隔での議論と同様に、到着数のカウントによっても仮想距離を定義することできる。Section 2 と同様の仮定の下で、時刻 t までに観測サーバーへ到着する単一感染源からの感染メール数を $N(t)$ とすると、$N(t)$ は以下のような Binomial Distribution となることがわかる。

$$P[N(t) = n] = \binom{l}{n} \alpha^k (1 - \alpha^{l-k}). \quad (6)$$

但し、$l = t/d$ とする。$E[N(t)] = t\alpha/d$、$Var[N(t)] = t\alpha(1-\alpha)/d$ なので、$\alpha = 1 - Var[N(t)]/E[N(t)]$ となるので、感染源までの仮想距離 m_β は下記のようにも定義できる。

Definition 2 (到着数による仮想距離).

$$m_\beta = \frac{\log\left(1 - Var[N(t)]/E[N(t)]\right)}{\log \beta}. \quad (7)$$

Remark 1. $Var[N(t)]/E[N(t)]$ は *index of dispersion of counts (IDC)* と呼ばれ、到着過程の性質を表す指標としてよく用いられる。*IDC* は到着過程の自己相関の大きさまで含めた指標となっている。到着間隔の相関まで含めた形で、*Definition 1* を拡張すると

$$m_\beta := \frac{\log\left(1 - nVar[\sum_{k=1}^n X_k]/\sum_{k=1}^n E^2[X_k]\right)}{\log \beta}. \quad (8)$$

このように定義することで、到着間隔に自己相関がある場合にも仮想距離が定義できる。到着間隔が *renewal process* の場合には、*(8)* は *Definition 1* と一致する。

Example 1 (複数の感染源). n 台の異なる独立な感染源からの感染メールが到着する場合を考える。i 番目の感染源からの時刻 t までの感染メールの到着数を $N_i(t)$、到達率を α_i、感染メールの送信間隔を d_i とする。するとトータルの感染源からの到達確率 $alpha$ は、次のように到着数の重み付け平均として推定されることがわかる。

$$\alpha = \frac{\sum_{i=1}^n E[N_i]\alpha_i}{E[N(t)]}.$$

特に、サーバーへの到達確率が 1 の感染源からの到着 $N_0(t)$ と *Poisson arrival* の *back ground* 到着 $N_b(t)$ がある場合には、

$$\alpha = \frac{E[N_0]}{E[N_0(t)] + E[N_b(t)]}.$$

back ground の *Poisson* 到着 $E[N_b(t)]$ が少ない場合には、$\alpha \approx 1$ となり、仮想距離は $m_\beta = 0$ となる。逆に $E[N_0(t)]$ が *back ground Poisson* 到着に比べて小さい場合には、$\alpha \approx 0$ となり、仮想距離は $m_\beta = \infty$ となる。

5 感染源に休止がある場合の仮想距離

感染源のマシンが電源オフになったり、ネットワークからログオフするなどの理由に一時的にウィルスの拡散が停止することがよく見られる。この場合には、観測サーバーで観測される感染ウィルスの到着間隔にゆがみが生じることになる。この影響を排除することを考える。

感染源に休止がある場合の観測される感染メールの到着間隔 X_n を次のようにモデル化する。

$$\begin{aligned} X_n &= Y_n + Z_n 1_{\{U_n=1\}} \\ &= Y_n + \bar{Z_n}. \end{aligned} \tag{9}$$

ここで Y_n は感染源がアクティブな場合の感染メールの到着間隔を表し、$\bar{Z_n}$ は感染源が休止期間に入った場合に到着間隔が長くなる効果を表し、感染源が停止されている期間を Z_n と表し、感染源が停止されている場合には $U_n = 1$、アクティブな場合には $U_n = 0$ とした場合に、$\bar{Z_n} = Z_n 1_{\{U_n=1\}}$ と表される。

Y_n が幾何分布なので、

$$\begin{aligned} E[X_n] &= E[Y_n] + E[\bar{Z_n}] \\ &= \frac{d}{\alpha} + E[\bar{Z_n}]. \end{aligned} \tag{10}$$

また、感染メールの送信間隔 Y_n、休止期間の長さ $\bar{Z_n}$ は独立であると仮定すると、

$$\begin{aligned} Var[X_n] &= Var[Y_n] + Var[\bar{Z_n}] \\ &= \frac{d^2(1-\alpha)}{\alpha^2} + Var[\bar{Z_n}]. \end{aligned} \tag{11}$$

(10) と (11) より α の推定値として以下の式を使うことができる。

$$\alpha = 1 - \frac{Var[X_n] - Var[\bar{Z_n}]}{(E[X_n] - E[Z_n])^2}. \tag{12}$$

また、この場合の仮想距離は、以下のように推定できる。

$$m_\beta = \log\alpha / \log\beta = \frac{1}{\log\beta} \log\left\{1 - \frac{Var[X_n] - Var[\bar{Z_n}]}{(E[X_n] - E[Z_n])^2}\right\}. \tag{13}$$

但し、$\bar{Z_n}$ の統計情報 $E[\bar{Z_n}]$ および $Var[\bar{Z_n}]$ があらかじめわかっている必要があるが、これは以下の手順により比較的容易に推定することができる。まず、到着間隔データの中で、有意に長い到着間隔を抜き出し、これを休止期間 Z_n と認定し、Z_n の期待値、分散および休止確率 $p := P\{U_n = 1\}$ を求める。ここで、U_n と Z_n が独立と仮定すると、$E[\bar{Z_n}] = pE[Z_n]$、および

$$\begin{aligned} Var[\bar{Z_n}] &= Var[Z_n 1_{\{U_n=1\}}] \\ &= E[Z_n^2 1_{\{U_n=1\}}] - E^2[Z_n 1_{\{U_n=1\}}] \\ &= pE[Z_n^2] - p^2 E^2[Z_n] \\ &= pVar[Z] + p(1-p)E^2[Z_n]. \end{aligned} \tag{14}$$

これらの式から $\bar{Z_n}$ の平均と分散が推定できる。

Example 2. 休止期間 Z_n が平均 $1/\mu$ の指数分布である場合には、$Var[Z_n] = 1/\mu^2$ なので次式により到達確率が推定できる。

$$\alpha = 1 - \frac{Var[X_n] - p(2-p)/\mu^2}{(E[X_n] - p/\mu)^2}. \tag{15}$$

また、この場合の仮想距離は

$$m_\beta = \frac{1}{\log\beta} \log\left\{1 - \frac{Var[X_n] - p(2-p)/\mu^2}{(E[X_n] - p/\mu)^2}\right\}. \tag{16}$$

として与えられる。

6 実観測データによる検証

仮想距離の概念を実際にインターネット上で観測されたコンピュータウィルスに適用した結果を示す。

図 2 から図 4 は会津大学のゲートウェーで実際に観測された感染メールの到着間隔を観測したデータである。観測ウィルスと観測日については表 1 参照していただきたい。ここでは、会津大学で多く観測された典型的なウィルスを特に多く観測された日を選んで分析している。

グラフ上の実線は平均値をもとにした指数分布の理論曲線である。Swen や Mimail といったウィルスについては、実線とよく似た実測値が得られていることがわかる。実際に観測したデータからは、$E^2[X_n]$ と $Var[X_n]$ は比較的近い値になっており、仮想距離 $m_{1/2}$ は大きな値であることがわかる。今回の場合は α が負になったため、仮想距離は無限大とした (表 1 参照)。実際、これらのウィルスは詳細に分析すると、外部ネットワークから会津大学への侵入を試みていたことがわかる。

一方、図 4 でわかるように、Lovegate は、他の二つのウィルスと明らかに異なる特性を持っていることがわかる。一定間隔でウィルスメールが観測されていたことがわかる。このことから、今回の感染源の Lovegate は、会津大学から非常に近い場所にいることが期待される。$m_{1/2} = 4.6$ 程度となっている (表 1 参照)。実際、この Lovegate は（残念ながら）会津大学内に感染源があることが明らかになったケースである。

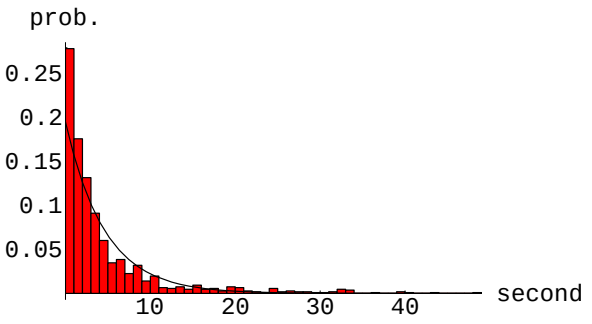

図 2: Intearrival time distribution of mails infected by Swen. The infected mails are detected at the gateway antivirus software of U. of Aizu.

表 1: 観測ウィルス

ウィルス名	観測期間	$E[X_n]$	$Var[X_n]$	α	$m_{1/2}$
Swen.A	2003/09/19 03:13:31 - 2003/09/22 23:40:52	311.386	337782.	-2.48368	∞
Mimail.R	2004/01/27 08:03:23 - 2004/01/30 14:59:48	98.2059	13398.1	-0.389209	∞
Lovegate.F	2003/07/03 13:24:08 - 2003/07/03 13:37:54	1.61004	2.48593	0.0410036	4.60811

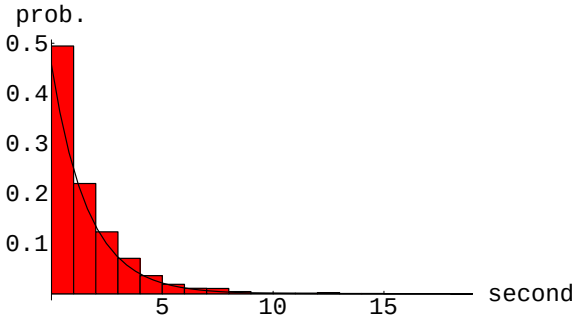

図 3: Intearrival time distribution of mails infected by Mimail. The infected mails are detected at the gateway antivirus software of U. of Aizu.

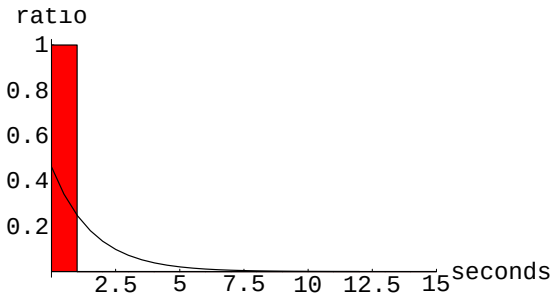

図 4: Intearrival time distribution of mails infected by Lovegate. The infected mails are detected at the gateway antivirus software of U. of Aizu.

7 仮想空間上への感染源の仮想位置のマッピング

単独の観測ポイントからの仮想距離だけでは、感染源を実ネットワーク上確定するのは、困難であるが、複数の観測ポイントにおける仮想距離を使い、仮想多次元空間上へ感染源をマップすることができる [8, 9]。この方法を使うことにより、感染源までの距離だけではなく、感染源の仮想的な位置や方向を仮想空間上に特定することができる。 感染源を特定することにより、predator [6] を感染源に近いところに集中的に配置するといった応用が考えられる。

8 おわりに

発信元を偽装したメールの到着間隔の確率的特性を利用することにより、発信源の探索方法を提案した。同様の手順は、メールだけではなく、IP レベルでの発信元アドレスの偽装などの場合にも応用可能である。特に、DDoS を装備したワームの位置の探索などに有効であると考えられる。

謝辞

本研究にあたって、データの提供／分析に協力をしていただいた会津大学林隆史助教授、海和建太氏および会津大学情報センターに感謝いたします。

参考文献

[1] Carey Nachenberg. Computer virus-antivirus coevolution. *Commun. ACM*, Vol. 40, No. 1, pp. 46–51, 1997.

[2] Prabhat K. Singh and Arun Lakhotia. Analysis and detection of computer viruses and worms: an annotated bibliography. *SIGPLAN Not.*, Vol. 37, No. 2, pp. 29–35, 2002.

[3] Harold Thimbleby, Stuart Anderson, and Paul Cairns. A framework for modelling Trojans and computer virus infection. *The Computer Journal*, Vol. 41, No. 7, pp. 445–458, 1998.

[4] K. G. Anagnostakis, M. B. Greenwald, S. Ioannidis, A. D. Keromytis, and D. Li. A cooperative immunization system for an untrusting internet. In *Proceedings of the 11th IEEE International Conference on Networks (ICON'03)*. IEEE, October 2003.

[5] K. Nunez, T. Gerace, and A. Hartman. The costly implications of consulting in a virus-infected computer environment. In *Proceedings of the 17th annual ACM SIGUCCS conference on User Services*, pp. 157–161. ACM Press, 1989.

[6] Hiroshi Toyoizumi and Atsuhi Kara. Predators: good will mobile codes combat against computer viruses. In *Proceedings of the 2002 workshop on New security paradigms*, pp. 11–17. ACM Press, 2002.

[7] Richard Durrett. *Probability: Theory and Examples*. Thomson Learning, 1991.

[8] T.S Eugene Ng and H.Zhang. Predicting internet network distance with cooridate-based approach. In *INFOCOM '02*, 2002.

[9] L. Tang and M. Crovella. Virtual landmarks for the internet. In *IMC-2003*, 2003.