2003年日本オペレーションズ・リサーチ学会
秋季研究発表会

確率モデルに基づいたコンピュータウィルスの挙動解析

小林尚志, 岡村寛之 (01013754), 土肥正 (01307065)
広島大学大学院工学研究科情報工学専攻

1. はじめに

コンピュータネットワークを基本とした現在の高度情報化社会において，インターネットは不可欠な情報伝達媒体として認識されているが，同時にコンピュータウィルス感染などの脅威に常にさらされている．近年，感染力などコンピュータウィルスに関する挙動の解析を行うという試みがなされている．Kephart and White [1] は Kill Signal と呼ばれるウィルスに対する警告を配信することを提案し，ウィルス拡散に関する時間的挙動を微分方程式を用いた数理モデルによって表現している．しかし，このような確定的な方法ではウィルスの感染除去に伴う不確実性の影響を無視しており，コンピュータウィルスの挙動に関する定量的評価を正確に行うことは困難である．そこで本稿では，確率モデルに基づいたコンピュータウィルスの挙動解析を行う．特に，ウィルスの拡散現象を連続時間マルコフ連鎖によって記述することのできる環境を想定し，ウィルス拡散現象に対する定量的評価尺度を導出する．

2. 微分方程式に基づいたウィルス拡散モデル

Kill Signal （以下 KS と記述）は「KS を受け取った端末が感染していた場合は感染を修復し，感染の可能性のある端末に KS を送る」という特徴を持ち，ウィルス感染に関する一種の警告を意味する．文献 [1] では，ウィルスに感染した端末台数と KS を保持している端末台数の時間的振る舞いを，以下の微分方程式で表現している．

$$\frac{dn(t)}{dt} = \beta n(t)\{K - n(t) - m(t)\} - \delta n(t) - \beta_r n(t)m(t), \quad (1)$$

$$\frac{dm(t)}{dt} = \beta_r m(t)\{K - m(t)\} + \delta n(t) - \delta_r m(t). \quad (2)$$

ここで，

K：感染する可能性のある総端末台数
$n(t)$：ウィルスに感染した端末台数
$m(t)$：KS を保持している端末台数
β：ウィルス感染率
δ：ウィルス除去率
β_r：KS 増加率
δ_r：KS 減少率

である．この微分方程式を解くことにより，コンピュータウィルスの拡散現象に関する時間的挙動の解析が可能となる．

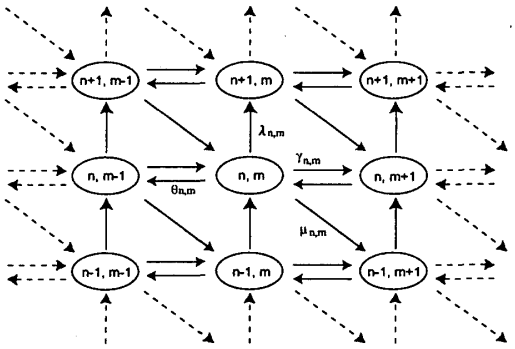

図 1: KS を伴うウィルスモデルの状態遷移図.

3. マルコフ連鎖に基づいたウィルス拡散モデル

Kephart and White [1] が提案した KS を考慮したウィルスモデルを確率モデルに拡張する．確率 $P_{n,m}(t)$ を時刻 t で感染した端末台数が n，KS を保持している端末台数が m である確率とすると，次の微分差分方程式が得られる．

$$\frac{dP_{n,m}(t)}{dt} = \lambda_{n-1,m}P_{n-1,m}(t) + \mu_{n+1,m-1}P_{n+1,m-1}(t) + \gamma_{n,m-1}P_{n,m-1}(t) + \theta_{n,m+1}P_{n,m+1}(t) - \nu_{n,m}P_{n,m}(t). \quad (3)$$

ここで $\nu_{n,m} = \lambda_{n,m} + \mu_{n,m} + \gamma_{n,m} + \theta_{n,m}$ である．この微分差分方程式において，状態 (n, m) から他の状態への遷移の推移率は以下のようになる．

1. ウィルス感染による状態 $(n+1, m)$ への推移率:

$$\lambda_{n,m} = \beta n(K - n - m). \quad (4)$$

2. ウィルスの除去による状態 $(n-1, m+1)$ への推移率:

$$\mu_{n,m} = \delta n + \beta_r mn. \quad (5)$$

3. KS の自己増殖による状態 $(n, m+1)$ への推移率:

$$\gamma_{n,m} = \beta_r m(K - n - m). \quad (6)$$

4. KS の自己消滅による状態 $(n, m-1)$ への推移率:

$$\theta_{n,m} = \delta_r m. \quad (7)$$

このとき，マルコフ連鎖の状態遷移図は図 1 のようになる．

次に確率モデルに基づいたウィルスの拡散過程を定量的に評価するための評価尺度を定義する．本稿では，感染台数に関する臨界レベル c を設定することで，ウィルスが死滅するこ

となく臨界レベルに達することをハザードとして定義し，すべてのコンピュータウィルスに対する定量的評価尺度を導出する．時刻 t でハザードが発生しない確率は，ウィルス感染した端末台数が c のときのウィルスの増加・除去率と KS の増加・減少率をすべて 0 と仮定した上で，微分差分方程式の解である状態確率 $\tilde{P}_{n,m}(t)$ を用いて，

$$R_c(t) = 1 - \frac{\sum_{m=0}^{K-c} \tilde{P}_{c,m}(t)}{\sum_{m=0}^{K-c} \tilde{P}_{c,m}(\infty)} \tag{8}$$

と表現される．また，ウィルスが死滅することなく臨界レベルに達するまでの平均時間 (Mean Time to Hazard: MTTH) は

$$\mathrm{MTTH}(c) = \int_0^\infty R_c(t)dt \tag{9}$$

により与えられる．

一方，ウィルス継続力に関してはウィルス感染端末台数が 0 に到達するまでの時間によって計測することができる．時刻 t でウィルスが死滅しない確率は

$$R_0(t) = 1 - \sum_{m=0}^{K} P_{0,m} \tag{10}$$

となり，ウィルスが死滅するまでの平均時間 (Mean time to Extinction: MTTE) は以下のようになる．

$$\mathrm{MTTE} = \int_0^\infty R_0(t)dt. \tag{11}$$

4. ウィルス拡散現象に関する評価尺度の計算法

次に再帰的な計算手続きによる MTTH(c) と MTTE の導出を行う．$\boldsymbol{A}_n$, $\boldsymbol{B}_n$, $\boldsymbol{C}_n$ をウィルス感染端末が n 台という条件の下で「感染端末が 1 台減少する」,「感染端末が変化しない（KS 保持端末台数が変化）」,「感染端末が 1 台増加する」という事象に対する確率行列とする．具体的に $\boldsymbol{A}_n$, $\boldsymbol{B}_n$, $\boldsymbol{C}_n$ の各要素（$[\boldsymbol{A}]_{ij}$ は行列 $\boldsymbol{A}$ の (i,j) 成分）は以下のようになる．

$$[\boldsymbol{A}_n]_{ij} = \begin{cases} \mu_{n,i}/\nu_{n,i} & \text{for } i = j+1 \\ 0 & \text{otherwise,} \end{cases} \tag{12}$$

$$[\boldsymbol{B}_n]_{ij} = \begin{cases} \theta_{n,i}/\nu_{n,i} & \text{for } i = j-1 \\ \gamma_{n,i}/\nu_{n,i} & \text{for } i = j+1 \\ 0 & \text{otherwise,} \end{cases} \tag{13}$$

$$[\boldsymbol{C}_n]_{ij} = \begin{cases} \lambda_{n,i}/\nu_{n,i} & \text{for } i = j \\ 0 & \text{otherwise.} \end{cases} \tag{14}$$

このとき，$\boldsymbol{F}_n$ をウィルス感染端末が n 台ある状態でウィルスが死滅することなくウィルス感染端末が $n+1$ 台に増加する確率を表す行列とすると

$$\boldsymbol{F}_0 = \boldsymbol{O}, \tag{15}$$

$$\boldsymbol{F}_n = (\boldsymbol{I} - \boldsymbol{A}_n\boldsymbol{F}_{n-1} - \boldsymbol{B}_n)^{-1}\boldsymbol{C}_n \tag{16}$$
$$\text{for } n = 1, \ldots, K-1$$

となる．また，行列 $\tilde{\boldsymbol{A}}_n$, $\tilde{\boldsymbol{B}}_n$, $\tilde{\boldsymbol{C}}_n$ をウィルス感染端末が n 台の条件の下で「感染端末が 1 台減少する」,「感染端末が変化しない（KS 保持端末台数が変化）」,「感染端末が 1 台増加する」までの期待時間を表す行列とすると

$$[\tilde{\boldsymbol{A}}_n]_{ij} = \begin{cases} \mu_{n,i}/\nu_{n,i}^2 & \text{for } i = j+1 \\ 0 & \text{otherwise,} \end{cases} \tag{17}$$

$$[\tilde{\boldsymbol{B}}_n]_{ij} = \begin{cases} \theta_{n,i}/\nu_{n,i}^2 & \text{for } i = j-1 \\ \gamma_{n,i}/\nu_{n,i}^2 & \text{for } i = j+1 \\ 0 & \text{otherwise,} \end{cases} \tag{18}$$

$$[\tilde{\boldsymbol{C}}_n]_{ij} = \begin{cases} \lambda_{n,i}/\nu_{n,i}^2 & \text{for } i = j \\ 0 & \text{otherwise} \end{cases} \tag{19}$$

となる．ここで，$\boldsymbol{M}_n$ をウィルス感染端末が n 台存在するという条件の下でウィルスが死滅することなく感染端末が $n+1$ 台に増加するまでの期待時間とすると，以下の漸化式によって算出できる．

$$\boldsymbol{M}_0 = \boldsymbol{O}, \tag{20}$$

$$\boldsymbol{M}_n = (\boldsymbol{I} - \boldsymbol{A}_n\boldsymbol{F}_{n-1} - \boldsymbol{B}_n)^{-1} \times (\tilde{\boldsymbol{A}}_n\boldsymbol{F}_{n-1}\boldsymbol{F}_n + \tilde{\boldsymbol{B}}_n\boldsymbol{F}_n + \tilde{\boldsymbol{C}}_n + \boldsymbol{A}_n\boldsymbol{M}_{n-1}\boldsymbol{F}_n) \tag{21}$$
$$\text{for } n = 1, \ldots, K-1.$$

上述の行列を用いて，臨界レベル c に対する MTTH(c) は

$$\mathrm{MTTH}(c) = \frac{\sum_{i=1}^{c-1} \boldsymbol{\alpha}\boldsymbol{F}_1 \cdots \boldsymbol{F}_{i-1}\boldsymbol{M}_i\boldsymbol{F}_{i+1} \cdots \boldsymbol{F}_{c-1}\boldsymbol{e}}{\boldsymbol{\alpha}\boldsymbol{F}_1 \cdots \boldsymbol{F}_{c-1}\boldsymbol{e}} \tag{22}$$

となる．ここで $\boldsymbol{\alpha}$ は初期時刻において KS を保持している端末の台数を表す確率ベクトル，$\boldsymbol{e}$ はすべての要素が 1 の列ベクトルである．

次に，MTTE の算出を行う．$\overline{\boldsymbol{F}}_n$ をウィルス感染端末が n 台ある状態でウィルス感染端末が $n-1$ 台に減少する確率を表す行列とすると，$\overline{\boldsymbol{F}}_n$ は以下の漸化式を満たす．

$$\overline{\boldsymbol{F}}_K = (0\ 1), \tag{23}$$

$$\overline{\boldsymbol{F}}_n = (\boldsymbol{I} - \boldsymbol{B}_n - \boldsymbol{C}_n\overline{\boldsymbol{F}}_{n+1})^{-1}\boldsymbol{A}_n, \tag{24}$$
$$\text{for } n = K-1, \ldots, 1.$$

また $\overline{\boldsymbol{M}}_n$ をウィルス感染端末が n 台存在するという条件の下で感染端末が $n-1$ 台に減少するまでの期待時間とすると，$\overline{\boldsymbol{M}}_n$ は以下の漸化式によって算出される．

$$\overline{\boldsymbol{M}}_K = (0\ 1/\mu_K), \tag{25}$$

$$\overline{\boldsymbol{M}}_n = (\boldsymbol{I} - \boldsymbol{B}_n - \boldsymbol{C}_n\overline{\boldsymbol{F}}_{n+1})^{-1} \times (\tilde{\boldsymbol{A}}_n + \tilde{\boldsymbol{B}}_n\overline{\boldsymbol{F}}_n + \tilde{\boldsymbol{C}}_n\overline{\boldsymbol{F}}_{n+1}\overline{\boldsymbol{F}}_n + \boldsymbol{C}_n\overline{\boldsymbol{M}}_{n+1}\overline{\boldsymbol{F}}_n), \tag{26}$$
$$\text{for } n = K-1, \ldots, 1.$$

上述の行列を用いて，MTTE は以下のようになる．

$$\mathrm{MTTE} = \overline{\boldsymbol{M}}_1. \tag{27}$$

参考文献

[1] Kephart, J. O. and White, S. R.: Measuring and modeling computer virus prevalence, *Proceedings of the 1993 IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 2–15 (1993).