Android端末を対象としたウイルス拡散モデルの評価

木下研究室　　古屋　智規 (200902880)

1　はじめに

近年，Android を狙ったウイルスが急増している．PC やクラウドとネットワークで連携しているため多くの情報を持っているので，狙われる危険性が高い．

Android ウイルスの感染経路は，主にアプリのダウンロードである．アプリが自由公開である点を悪用され，正規品に混入させたり，ランキングや口コミの情報操作で多くの端末にダウンロードさせることが可能である．

今まで，PC を対象としたウイルスの評価がされてきた．しかし，PC と Android では感染経路が異なり，Android から PC への感染も起こる．それらから，従来の PC を対象としたモデルとは状態遷移が変わると考えられる．本研究では，従来されてきた研究に Android の感染について導入し，新たにウイルス拡散モデルの評価を導いていく．

2　従来手法

2.1　マルコフ過程

PC のウイルス拡散モデルには，マルコフモデルが多く用いられている．

マルコフ過程の基本概念はシステムの “状態” と状態の “遷移” であり，状態遷移を考えるうえで有効なモデルである．

2.2　NHCTMC を用いた拡散モデル

総 PC 台数を N とし，ウイルスの感染台数，駆除台数の状態遷移をマルコフ性を用いてモデル化する．

ウイルスの感染率、駆除率をそれぞれ仮定し，時刻 t においてウイルスに感染していない PC が i 台，感染している PC が j 台である確率を確率ベクトルで表す．総 PC 台数の K 台以上がウイルスに感染している状態をハザードとして定義，先の確率から，時刻 t における情報システムの信頼度 $R(t)$ を求める．

感染率 $\lambda\ (t)$，信頼度 $R(t)$ にそれぞれ数値例を代入し，時間に対する感染率，信頼度をグラフ化する．

3　提案手法

従来手法では PC だけのモデルについて，時間に対するシステムの信頼度を過渡的な状態を表している．本研究で考えるモデルは，従来手法のモデルと変わってくると考えられる．

そこで，まずは定常状態での期待感染台数を従来手法，提案手法を用いて求めていくことを目標とする．

3.1　PC，Android の感染経路

PC と Andriod のウイルス拡散方法には感染経路の違いがあり，PC は主にメール，添付ファイル．一方，Android はアプリのダウンロードである．

ここで，PC，Android 間でもデータ通信，PC に Android を接続することにより異なる端末間での “2 次感染” が起こる．PC 間感染，Android 間感染のように，同じ端末間での感染については従来手法で評価できるが，“2 次感染” を考慮した場合，従来手法とは違った状態遷移，評価になると考えられる．

3.2　PC，Android のウイルス拡散モデル

従来手法のモデルでは，今回考える 2 つの端末間での 2 次感染を含むモデルを表すことには適していない．そこで，新たに 2 次感染を含めたモデルを提案する．

マルコフモデルを用いて，PC と Android による 2 次感染を含むウイルス拡散の状態遷移を図 1 のようにモデル化する．ここで，総台数を PC，Android それぞれ N 台，M 台とする．また，定常状態を考慮して PC，Android，Android から PC への感染率をそれぞれ λ_p，λ_a，λ_{ap} のポアソン分布，PC，Android の駆除率をそれぞれ μ_p，μ_a の指数分布とする．

定常状態におけるそれぞれの状態の確率を求め，2 次感染を含めたモデルの感染台数の期待値を算出する．

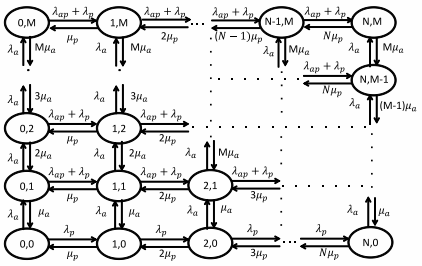

図 1: ウイルス感染台数の状態遷移図

4　評価方法

2 次感染を含めたモデルの期待感染台数 $E(N_{ap})$ を提案手法により求める．

同様に PC，Android の期待感染台数 $E(N_p)$，$E(N_a)$ を従来手法のモデルにより定常状態であることを考慮して算出する．

結果より，2 次感染が起こることで定常状態における期待感染台数がどのように変化しているのか比較検討を行う．