마코프 체인을 이용한 모바일 악성코드 예측 모델링 기법 연구

김종민* · 김민수* · 김귀남**

요 약

모바일 악성코드는 웜에 의한 전파가 대표적이며, 웜의 확산 특징을 분석하기 위한 모델링 기법들이 제시되었지만 거시적인 분석만 가능하였고 특정 바이러스, 악성코드에 대해 예측하기는 한계점이 있다. 따라서 본 논문에서는 과거의 악성코드 데이터를 활용하여 미래의 악성코드의 발생을 예측 할 수 있는 마코프 체인을 기반으로 한 예측 방법을 제시하였다. 마코프 체인 예측 모델링에 적용할 악성코드 평균값은 전체 평균값, 최근 1년 평균값, 최근 평균값(6개월)의 세 가지 범위로 분류하여 적용하였고, 적용하여 얻어진 예측 값을 비교하여 최근 평균 값(6개월)을 적용하는 것이 악성코드 예측 확률을 높일 수 있음을 확인하였다.

Research on Mobile Malicious Code Prediction Modeling Techniques Using Markov Chain

JongMin Kim* · MinSu Kim* · Kuinam J. Kim**

ABSTRACT

Mobile malicious code is typically spread by the worm, and although modeling techniques to analyze the dispersion characteristics of the worms have been proposed, only macroscopic analysis was possible while there are limitations in predicting on certain viruses and malicious code. In this paper, prediction methods have been proposed which was based on Markov chain and is able to predict the occurrence of future malicious code by utilizing the past malicious code data. The average value of the malicious code to be applied to the prediction model of Markov chain model was applied by classifying into three categories of the total average, the last year average, and the recent average (6 months), and it was verified that malicious code prediction possibility could be increased by comparing the predicted values obtained through applying, and applying the recent average (6 months).

Key words : Markov Chain, Mobile, Malicious Code, Prediction

접수일(2014년 6월 02일), 수정일(1차: 2014년 6월 15일),
게재확정일(2014년 6월 16일)

* 경기대학교 산업보안학과
** 경기대학교 융합보안학과

1. 서 론

2004년 Cabir의 출현한 이후 다양한 모바일 악성코드가 발견되고 있으며, 점차 다양한 변종 악성코드를 유포하여 모바일기기에 대한 보안위협수준이 증가되고 있다[1].

모바일 기기의 플랫폼OS의 경우 UNIX를 기반으로 사용되어 루트권한을 획득하지 못한다면 악성코드가 사용할 수 있는 파일의 권한이 없어서 악성코드로부터 안전하였다. 하지만 문자 및 블루투스, 인터넷 서비스, 그리고 모바일 앱 등 다양한 경로를 통해 시스템의 보안을 무력화 시키고 있다[2]. 이렇게 보안을 무력화 시킨 모바일 기기에 접속해 저장되어 있는 개인신상정보등이 유출되면 심각한 피해를 입을 수 있다.

이러한 모바일 악성코드의 증가에도 불구하고 현재 모바일 악성코드 예측모델에 관한 연구가 미흡한 실정이다.

따라서 본 논문에서는 모바일 악성코드 발생 데이터를 이용하여 마코프 체인 모델링에 적용시켜 모바일 악성코드에 대한 예측기술을 연구 한다.

2. 관련연구

2.1 모바일 악성코드

모바일 악성코드는 악의적인 목적을 가지고 이익을 달성하기 위해 스마트폰OS를 감염시키며, Repackaging, Malvertizing, Browser Attacks, Update Attacks, Drive-by-Download등 과 같은 감염의 기술이 일반적으로 사용된다 [3].

<표 1>은 모바일 기기의 OS별 주요 악성코드를 나열한 것이다.

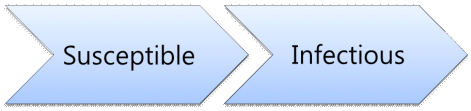
<표 1> 모바일 기기 OS별 주요 악성코드현황[4]

OS	악성코드명	설명
Android	SMSRelicator	문자메시지를 이용자 몰래 실시간으로 특정 이용자에게 유출
	SMSSend	문자 메시지를 통한 과금 발생 유도 등
	Snake	유호 앱인 GPSSpy T류Snake가 설치된 스마트폰 위치확인, 이용자의 GPS 정보를 특정 서버로 전송
	Ewalls	스마트폰 내의 개인정보 또는 단말기 정보를 수집해 특정서버로 전송, 다수의 유사 프로그램 발생
	Geinimi	중국에서 발견, 개인정보를 특정 서버로 전송
Windows Mobile	TreDial	국제전화를 무단으로 발신해 원치 않는 과금 유발
	Duts	윈도우 모바일 최초의 바이러스, 실행파일 감염, 개념증명 자이러스
iOS	Privacy.A	감염된 아이폰에서 무선랜을 접속하는 경우, 개인정보(문자메시지, 이메일 등)를 원격으로 전달
	Agent.535552.F	아이폰 탈옥프로그램으로 위장한 정보유출형 악성코드, 구글토크, MSN메신저, 야후 등의 서비스에 로그인 할 때 ID와 패스워드 등의 계정 정보 유출)
	LKE Worm	아이폰 최초의 악성코드, 배경화면 변경, 탈옥기기에서 동작

2.2 기존 예측 모델링 기법

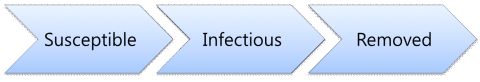
초기의 모델링 기법 연구는 바이러스에 대한 모델링 기법으로 시작되어 데이터의 흐름 또는 정보의 흐

름이 바이러스 전파에 매우 많은 영향을 미칠 것으로 가정하여 이를 바이러스 모델링에 적용하였다. 각 모델링 기법의 한계점을 알아보면 Epidemic모델링의 경우 (그림 1)처럼 감염된 하나의 호스트에 의해 접속이 성공하면 즉시 감염이 된 것처럼 모든 상태를 감염된 상태(Infectious)와 취약한 상태(Susceptible) 두 가지로 표현하는 모델링이며 웜이 전송되는 시간 등은 고려되지 않았다. 또한 보안패치 및 백신프로그램 최신번전 적용 등 인간에 의한 대응책이 고려되지 않았다[5].



(그림 1) SI모델

General Epidemic Model (Kermack-MeKendrick Epidemic Model)은 (그림 2)처럼 SI 모델링 기법의 단점을 보완, 취약점이 제거된 상태(Removed)를 표현할 수 있는 모델링 기법으로서 SIR (Susceptible-Infectious-Removed)이라고 불린다. 하지만, 이 모델링 기법은 (그림 3)와 같이 취약한 호스트가 웜에 감염되기 전에 취약점이 조치된 상태의 표현이 불가능하다[6].



(그림 2) General Epidemic Model

(그림 3) 감염 전, 취약점 조치 상태

이렇듯 기존의 모델링들은 바이러스에 대한 거시적인 분석만 가능하여 왔으며, 예측에 대한 한계점을 가지고 있다.

2.3 마코프 체인

마코프 체인은 과거의 동적 특성을 분석하여 미래에 있을 변화를 예측하기 위한 수학적 기법이다[7]. 날씨를 예로 들어 설명하면 오늘의 날씨가 맑았다고 해서 내일의 날씨도 맑다고 할 수 없다. 확률적으로는 맑은 날, 흐린날, 비가 오는 날이 될 수도 있다. 이것을 비결정 시스템이라고 하고 이러한 문제를 해결하기 위해 사용된다[8].

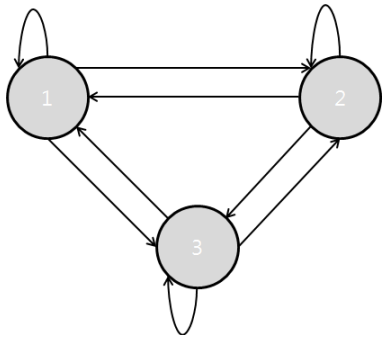
시간에 따라 변화하는 확률 변수의 경우 확률 변수는 $X(t)$로 표현된다. 따라서 마코프 체인을 $X(t)$라 하면 임의의 시간인 $t_1 < t_2 < .....t_k < t_{k+1}$에 대해 $X(t)$가 이산값일 경우에는 마코프 체인은

$$P[a < X(t_{k+1}) = x_{k+1} | X(t_k) = x_k, ..., X(t_1) = x_1] \quad (식\ 1)$$
$$= P[X(t_{k+1}) = x_{k+1} | x(t_k) = x_k]$$

로 기술된다. t_k는 현재, t_{k+1}은 미래, $t_1,...,t_{k-1}$은 과거의 시점을 말한다.

$X(t)$는 시계열적인 특성으로 나열된 것인데 이러한 과정을 확률 과정이라고 한다[2].

이러한 마코프 모델은 특정 상태에서 다른 상태로 전이 되는 형태에 따라 (그림 4)의 에르고딕(ergodic) 모델로 표현된다[9].



(그림 4) 에르고딕(ergodic)모델

3. 모바일 악성코드 예측 모델링

3.1 악성코드 예측 모델링

마코프체인은 임계값의 바탕으로 상태집합을 정의하고, 초기확률, 전이행렬을 계산 후 초기확률과 전이행렬을 이용하여 확률 값을 구한다

① 상태집합(S) : 악성코드 예측 모델링에서 상태란 악성코드가 발생하는 빈도수의 범위를 말하며, 적절한 임계값을 설정하여 상태들을 집합으로 정의한다.

② 초기확률 : 임계값으로 정의된 상태에서 초기에 발생할 수 있는 악성코드 확률로서 (식 2)와 같이 정의한다.

$$P(S_1,S_2,...,S_n)=P(\frac{a}{F},\frac{b}{F},...,\frac{c}{F}) \quad (식\ 2)$$

여기서 a,b,c는 각 상태 $(S_1,S_2,...,S_n)$의 악성코드 횟수이고 F는 a,b,c의 합이다. 또한 초기 확률의 총합은 1이 되어야 한다.

$$\sum_{i=1}^{n}P(S_i) = 1(S는\ 상태) \quad (식\ 3)$$

③ 전이행렬 : 임계값으로 정의된 상태간의 전이상태를 확률로 나타낸다. 데이터와 상태집합과 집합과 매칭하여 상태들을 열거한다. 그리고 열거된 하나의 상태에서 다른 상태로의 전이 횟수를 구한후 이를 전이 행렬로 나타내는 것이다. 각 행의 합은 1이 되어야 하며 (식 3)은P 의 전이행렬로서 (식 4)을 만족시킨다.

$$P=\begin{pmatrix} P_{11} & P_{12} & P_{13}\cdots & P_{1n} \\ P_{21} & P_{22} & P_{23}\cdots & P_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ P_{n1} & P_{n2} & P_{n3}\cdots & P_{nn} \end{pmatrix} \quad (식\ 4)$$

$$\sum_{j=1}^{n}P_{1j}=1,\sum_{j=1}^{n}P_{2j}=1,...,\sum_{j=1}^{n}P_{nj}=1,P_{ij}\geq 0 \quad (식\ 5)$$
$$\sum_{j=1}^{n}P_{1j}=1,i=1,2,...,n$$

④ 악성코드 발생 확률 : 마코프 체인을 사용하여 (식5)로 정의 된다

$$P(S_k)=\sum_{i=1}^{n}P(S_i)P_{ik} \quad (식\ 6)$$

$P(S_i)$: 초기확률,

P_{ik} : 전이행렬

⑤ 악성코드 발생 예측 식 : 기존 논문들은 악성코드 건수를 확률 값과 악성코드 건수의 중간 값을 이용하여 발생 빈도수를 산출 하였지만, 본 논문에서는 악성코드 발생 예측할 때 다양한 평균값을 적용하여 산출 하였다.

$$예측발생건수=\sum_{i=1}^{n}P(S_i)\,WM(S_i) \quad (식\ 7)$$

$$예측발생건수=\sum_{i=1}^{n}P(S_i)\,YM(S_i) \quad (식\ 8)$$

$$예측발생건수=\sum_{i=1}^{n}P(S_i)\,HM(S_i) \quad (식\ 9)$$

$n=$ 발생상태집합의상태수

$P(S_i)$: 발생확률

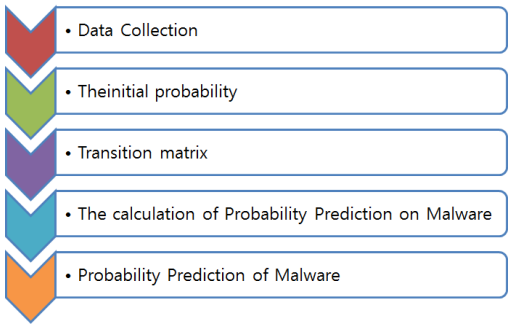
$WM(S_i)$: 발생건수의전체평균값
$YM(S_i)$: 최근1년간발생건수의평균값
$HM(S_i)$: 최근6개월간발생건수의평균값

3.2 악성코드 예측 프로세스

본 논문에서는 모바일 악성코드의 예측 모델링을 구성하였다. (그림 5)는 마코프 체인을 적용한 모바일 악성코드 예측 모델의 처리과정을 나타낸 프로세스이며, 크게 5단계(데이터 수집, 상태설정, 전이행렬, 악성코드의 초기 확률 예측의 계산, 악성코드 확률예측)로 이루어진다.

1단계인 데이터 수집에서는 모바일 악성코드 발생에 대한 데이터를 수집하여 통계화 한다. 2단계인 상태집합의 단계에서는 악성코드의 발생한 값들의 범위를 설정한다. 3단계인 전이행렬에서는 상태집합에서 발생빈도의 범위 데이터를 이용하여 전이행렬을 구한다. 4단계인 악성코드의 초기확률(π 벡터)에서는 악성코드가 초기상태에 발생할 수 있는 확률을 구한다. 마지막 5단계 악성코드 확률예측 단계에서는 전 단계

에서 구한 전이행렬과 초기확률 값을 통해 미래에 발생할 수 있는 악성코드의 확률을 예측 할 수 있다.



(그림 5) 모바일 악성코드 예측 프로세스

4. 예측 모델링 적용

4.1 모바일 악성코드 발생건수

<표 2>는 A社에서 발표한 모바일 악성코드 발생건수로서 2011년 1월부터 2013년 7월 까지 발생한 건수를 나타낸 것이다.

<표 2> 모바일 악성코드 발생건수[10]

구분	2011	2012	2013
1월	5	2,112	43,109
2월	9	4,578	83,868
3월	21	5,233	79,651
4월	4	2,053	239,471
5월	14	4,871	108,088
6월	59	3,848	92,732
7월	107	22,189	86,423
8월	88	29,591	
9월	158	38,427	
10월	710	76,789	
11월	6,089	48,261	
12월	1,095	24,747	

4.2 상태집합

모바일 악성코드의 발생 빈도수는 <표 2>와 같으며, (수집된 데이터를 기반으로 발생 단위 빈도를 동등한 전이율을 나타내기 위해서 다음과 같이 범위를 설정하였다.

▷ 임계값의 범위

S_1 : $0-1{,}000$, S_2 : $1{,}001-10{,}000$,

S_3 : $10{,}001-100{,}000$, S_4 : $100{,}000-200{,}000$,

S_5 : $200{,}001-$

▷ 임계값의 범위

$$S = \{S_1, S_2, S_3, S_4, S_5\}$$

2011년 1월부터 2013 7월까지 악성코드 발생빈도를 정의된 임계값의 범위를 <표 2>에 매칭하여 상태를 나열한다.

$S_1\ S_1\ S_1\ S_1\ S_1\ S_1\ S_1\ S_1\ S_1\ S_1\ S_2\ S_2$

$S_2\ S_2\ S_2\ S_2\ S_2\ S_2\ S_3\ S_3\ S_3\ S_3\ S_3\ S_3$

$S_3\ S_3\ S_3\ S_5\ S_4\ S_3$

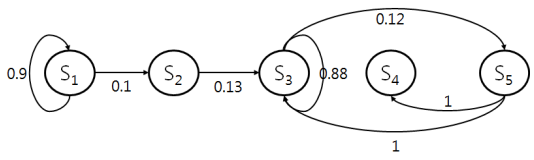
나열된 상태로부터 각각의 상태

$\{S_1, S_2, S_3, S_4, S_5\}$에서 다른 상태로의 전이 횟수를 구하고, 이를 바탕으로 앞의 (식 4)를 이용하여 전이확률로 바꾼 후, 전이행렬로 표현하면 (식 9)과 같이 나타난다.

$$\begin{array}{c} \\ S_1 \\ S_2 \\ S_3 \\ S_4 \\ S_5 \end{array} \begin{array}{c} \begin{array}{ccccc} S_1 & S_2 & S_3 & S_4 & S_5 \end{array} \\ \begin{pmatrix} 9 & 1 & 0 & 0 & 0 \\ 0 & 7 & 1 & 0 & 0 \\ 0 & 0 & 8 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

$$\begin{array}{c} \\ S_1 \\ S_2 \\ S_3 \\ S_4 \\ S_5 \end{array} \begin{array}{c} \begin{array}{ccccc} S_1 & S_2 & S_3 & S_4 & S_5 \end{array} \\ \begin{pmatrix} 0.9 & 0.1 & 0 & 0 & 0 \\ 0 & 0.87 & 0.13 & 0 & 0 \\ 0 & 0 & 0.88 & 0 & 0.12 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \end{array} \quad (식\ 9)$$

(식 9)의 상태전이행렬의 각 행의 합은 확률 값이므로 합이 1이 되어 (식 5)를 만족하고 상태 전이 확률을 다이어그램으로 나타내면 (그림 6)과 같다.



(그림 6)상태전이 다이어그램

4.3 초기확률

본 논문에서 초기확률을 구하기 위해서 마지막 5개월인 2013년 2월 ~ 6월의 위협건수를 적용 하였다. (식 2)를 이용하여 마지막 5개월에 발생한 악성코드의 초기확률을 구하면 다음과 같다.

▷ 보안 위협 발생 건수

83,868, 79,651, 239,471, 108,088, 92,732 =

S_3, S_3, S_5, S_4, S_3

▷ 초기확률

$$P\ (S_1:0 \quad S_2:0 \quad S_3:3 \quad S_4:1 \quad S_5:1)$$
$$= P\ (0 \quad 0 \quad 0.6 \quad 0.2 \quad 0.2)$$

4.4 악성코드 발생 확률

(식 2), (식 4)를 이용하여 구해진 초기확률과 전이행렬을 이용하여 그 값을 구하면 악성코드 발생 확률을 구할 수 있다.

$$(0 \ \ 0 \ \ 0.6 \ \ 0.2 \ \ 0.2)\begin{pmatrix} 0.9 & 0.1 & 0 & 0 & 0 \\ 0 & 0.87 & 0.13 & 0 & 0 \\ 0 & 0 & 0.88 & 0 & 0.12 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \quad (식\ 10)$$

$$= (0 \ \ 0 \ \ 0.73 \ \ 0.2 \ \ 0.07)$$

4.5 악성코드 발생 예측

구해진 (식 10)에 의해 다음 달 모바일 악성코드 발생 확률은 S_3일 때 0.73으로 가장 높게 나타났다. 다음 달에 발생할 악성코드의 건수를 예측하기 위해 발생 확률 값에 전체의 평균 값, 최근1년 간 평균값, 최근 평균값을 적용하였다.

▷ 전체 평균 값

2011년 ~ 2013년 6월까지 발생한 악성코드의 평균값을 (식 7)을 이용하여 예상 발생 건수를 구한다.

$$M(S_i) = 30,599$$
$$\text{예측발생건수} = \sum_{i=1}^{n} P(S_i)\, WM(S_i)$$
$$= 0.73 * 30,599$$
$$= 22,337.27$$

▷ 최근 1년간 평균 값

최근 1년간 발생한 악성코드의 평균값을 (식 8)을 이용하여 예상 발생 건수를 구한다.

$$Y(S_i) = 73,910$$
$$\text{예측발생건수} = \sum_{i=1}^{n} P(S_i)\, YM(S_i)$$
$$= 0.73 * 73,910$$
$$= 53,954.3$$

▷ 최근 평균 값

2013년 2월~2013년 7월까지 최근 6개월간 발생한 악성코드의 평균값을 (식 9)을 이용하여 예상 발생 건수를 구한다.

$$H(S_i) = 12,762$$

$$\text{예측발생건수} = \sum_{i=1}^{n} P(S_i)\, YM(S_i)$$

$$= 0.73 * 79,263$$
$$= 88,156.26$$

S_4일 때 0.2, S_5일 때 0.07으로 예측할 수 있다. 즉 다음 달 모바일 악성코드 발생 건수는 S_3 상태인 10,001 ~ 100,000 사이에서 발생할 것으로 예측된다. 본 논문은 다음 달에 발생할 악성코드 발생건수를 예측하기 위해 발생 확률 값을 적용하여 예상 발생 건수를 (식 6)을 이용해서 구한다. 여기서$M(S_i)$ 값은 마지막 5개월의 발생건수 합의 평균값이다.

$$\text{예측발생건수} = \sum_{i=1}^{n} P(S_i) M(S_i)$$

$$= 0.73 * 120,762$$
$$= 88,156.26$$

악성코드의 건수를 예측할 결과 전체 평균값일 때 약 22,337건, 최근 1년간 평균값일 때 약 53,954건, 최근 평균값일 때 약 86,423건으로 예측 되었고 실제 2013년 7월에 발생한 모바일 악성코드 발생 건수는 약 88,156건으로 나왔으며, 실제 2013년 7월에 모바일 악성코드 발생건수는 86,423건이 발생했다.

4.6 평균값의 변화에 따른 악성코드 발생건수 분석

<표 3>은 모바일 악성코드의 발생건수를 마코프 체인 모델링에 적용하여 악성코드 발생 확률을 산출하여 악성코드를 예측하기 위해 평균값의 변화를 주어 평균값에 따라 발생한 예측 건수이다. 악성코드의 발생건수 평균값에 대해 변화를 주자 악성코드의 예측 건수가 변화하는 것으로 나타났으며, 최근 평균값(6개월)을 적용하였을 때, 실제 발생건수와 유사하게 나타났음을 알 수 있다.

<표 3> 발생예측 건수와 실제발생 건수 비교

평균 분류	악성코드 예측건수	실제발생 건수	차이 (±)
전체평균	22,377	86,423	64,046
최근1년 평균	53,954	86,423	32,469
최근평균 (6개월)	88,156	86,423	1,733

5. 결 론

본 논문에서는 마코프 체인을 이용하여 모바일 악성코드 예측 모델링을 제안하였다. 또한 실제 일어난 악성코드 데이터를 이용하여 제안한 모델에 적용하여 예측 확률을 산출하고, 발생할 수 있는 악성코드 건수를 예측하였다.

악성코드의 발생건수 예측에 적용할 평균값을 전체 평균값, 최근 1년간 평균값, 최근평균값(6개월), 3가지로 나누어 악성코드의 발생건수를 예측해 보았다. 그 결과 최근평균값(6개월)을 적용하는 것이 실제 악성코드가 일어난 건수가 유사하였다. 이 결과 마코프 체인을 이용하여 예측 모델링을 적용하면 악성코드에 대한 건수를 예측할 수 있으므로 모바일 악성코드 발생에 대한 예방정책을 설정하여 피해를 최소화 할 수 있을 것이라 기대된다. 하지만 마코프 체인으로 나온 결과는 가까운 미래는 예측할 수 있으나 먼 미래는 예측하기 어려운 점이 있다. 그리고 데이터의 시간별, 단위별 등 세부적인 단위별 데이터를 이용한다면 더욱 정확한 예측을 할 수 있을 것이다. 그러므로 향후 먼 미래의 예측과 세부 단위별 데이터를 이용하여 이러한 단점을 보완한 연구가 필요하다.

참고문헌

[1] Qiang Yan, Robert H. Deng, Yingjiu Li, Tieyan Li, "On the Potential of Limitation-oriented Malware Detection and Prevention Techniques on Mobile Phones", International Journal of Security and Its Applications, Vol. 4, No. 1, 2010.

[2] 김호연, 장성수, 최영현, 정태명, "모바일 환경에서 악성코드 분석을 위한 효율적 동적 분석기법 연구", 한국정보처리학회 2011년도 제35회 춘계학술발표대회, 2011.

[3] Seo, Seung-Hyun, Aditi Gupta, Asmaa Mohamed Sallam, Elisa Bertino, Kangbin Yim, "Detecting mobile malware threats to homeland security through static analysis", Journal of Network and Computer Applications, Volume 38, pp. 43-53, 2014.

[4] 유효선, "모바일오피스 구현- 보안대책마련'최우선'", Network Times, 2011. 3.

[5] Cliff Changchun Zou, Weibo Gong, Don Towsley "Code Red Worm Propagation Modeling and Analysis", Conferrence on Computer and Communications Security, 2002.

[6] D. J. Deley and J. Gani, "Epidemic Modeling: An Introduction", Cambridge university Press, 1999.

[7] Charles M. Grinstead, "Introduction to Probability:Second Revised Edition", American MathematicalSociety, pp405-406, 1997.

[8] 박원형, 김영진, 이동휘, 김귀남, "마코브 체인을 이용한 Mass SQL Injection 웜 확산 예측에 관한 연구", 정보보안논문지, 제8권 제4호, pp. 173-181, 2008.

[9] 한학용, "패턴 인식 개론", 한빛미디어, pp432-438, 2009.

[10] http://www.ahnlab.com/kr/site/securitycenter/asec/asecReportList.do

[저 자 소 개]

김 종 민 (Jong-Min Kim)

2012년 현재 경기대학교 산업보안학과 박사과정

email : dyuo1004@gmail.com

김 민 수 (Min-Su Kim)

2004년 2월 컴퓨터공학사
2012년 2월 경호안전학석사
2012년 현재 경기대학교 산업보안학과 박사과정

email : fortcom@hanmail.net

김 귀 남(Kuinam J. Kim)

미국 캔자스대학(학사)
미국 콜로라도주립대학(석사)
미국 콜로라도주립대학(박사)
현재 경기대학교 융합보안학과 교수

email : harap123@daum.net