한국시뮬레이션학회 논문지
Vol. 15, No. 4, pp. 1-10 (2006. 12)

인공생명 기반의 웜바이러스 모델링 및 시뮬레이션 방법론

오지연[1] · 유용준[2†] · 채수환[2] · 지승도[2]

Worm Virus Modeling and Simulation Methodology Using Artificial Life

Jiyeon Oh · Yongjun You · Soohoan Chae · Sungdo Chi

ABSTRACT

Computer virus modeling and simulation research has conducted with focus on the network vulnerability analysis. But computer virus shows the biological virus characters such as proliferation, reproduction and evolution. Therefore it is necessary to research the computer virus modeling and simulation using the Artificial life technique. The approach of computer modeling and simulation using Artificial life provides the analysis method about the effects on the network by computer virus and the behavior mechanism of computer virus. Hence this paper proposes the methodology of computer virus modeling and simulation using Artificial life, which is effected to contribute the research on the computer virus vaccine.

Key words : Worm virus modeling, Artificial life

요 약

컴퓨터 바이러스의 모델링 및 시뮬레이션에 관한 연구는 주로 네트워크 취약성 분석에 초점이 맞추어져 있었다. 그러나 컴퓨터 바이러스는 생물학적인 관점에서 분석되어 질 수 있다고 생각하여, 인공생명 기술을 이용하여 컴퓨터 바이러스를 분석하였다. 이 연구를 통해 컴퓨터 바이러스로 인해 네트워크에 미칠 영향과 행동 메커니즘을 이해할 수 있을 것이다. 본 논문에서는 인공생명을 이용한 컴퓨터 바이러스의 모델링 및 시뮬레이션 방법론을 제안한다. 이를 통해 컴퓨터 바이러스 백신의 연구에도 영향을 줄 수 있다.

주요어 : 웜 바이러스 모델링, 인공생명

1. 서 론

최근 컴퓨터 바이러스는 다른 프로그램을 감염시키지 않고 네트워크를 통해 바이러스 자신을 복제하여 전파하는 웜 바이러스의 형태로 발전하는 추세를 보인다.[5] 지난 2003년에 일어난 '1.25 인터넷 대란'은 전 세계적인 인터넷 마비사태로 웜 바이러스의 위험성을 극명히 보여주었다. 또한 웜 바이러스에 대한 연구의 필요성을 각인시켰다. 그러나 기존의 연구는 웜 바이러스가 네트워크 취약성에 미치는 영향에 대한 분석에 대한 것이었다.[6] 따라서 본 논문에서는 컴퓨터 바이러스 중 최근 그 피해의 심각성이 대두되고 있는 웜 바이러스의 시뮬레이션을 위해서 인공생명기반의 웜 바이러스 모델을 제시한다.

컴퓨터 바이러스는 1970년대부터 제작되기 시작하였으며, 컴퓨터 바이러스 자신을 복제하기 위해서 다른 숙주 파일이나 부트 영역을 변경하는 악성 프로그램으로 정

2005년 12월 31일 접수, 2006년 3월 14일 채택
1) (주) 챈스아이
2) 한국항공대학교 컴퓨터공학과
주 저 자 : 유용준
교신저자 : 오지연
E-mail; ilog21c@hau.ac.kr

의한다.[2] 컴퓨터 바이러스에 감염된 숙주 객체는 컴퓨터 바이러스의 악성 코드를 완전한 복사본으로 포함하고 있기 때문에 숙주 파일이나 부트 영역이 실행되면 컴퓨터시스템에 존재하는 다른 객체는 컴퓨터 바이러스에 감염된다. 따라서 컴퓨터 바이러스는 프로그램을 감염시키고 복제하여 전파하는 특징을 갖는다. 이러한 특징은 성장, 증식, 진화하는 생물학적 바이러스와 유사하기 때문에 컴퓨터 바이러스를 인공생명체로 인식할 수 있다. 따라서 인공생명기반의 컴퓨터 바이러스 모델링을 통하여 컴퓨터 바이러스의 생명체적인 메커니즘을 분석함으로써 컴퓨터 바이러스의 감염 및 확산을 효과적으로 분석 할 수 있다. 이에 따라 외국에서는 Eugene H. 등을 중심으로 인공생명기반의 컴퓨터 바이러스에 관련된 연구가 진행 중이다[3,4].

전 세계적인 정보화와 인터넷의 보급은 컴퓨팅 환경의 변화와 더불어 정보통신에 대한 의존도를 증대시켰다. 그 결과, 정보통신 기반구조에 대한 침해는 개별 서버 및 국가적, 경제적, 사회적 마비를 통하여 막대한 피해를 야기한다. 이는 정보통신 시스템 자체의 버그, 부적절한 구성설정, 개방형 인터넷 기반구조 등에 따른 취약성을 이용한 해킹 뿐 아니라, 컴퓨터 바이러스에 대한 피해도 포함한다[1].

2. 인공생명기반의 웜 바이러스 모델링 및 시뮬레이션 접근 방법

인공생명기반의 웜 바이러스의 모델링 및 시뮬레이션을 위한 접근 방법은 그림 1과 같다.

2.1 1단계 : 개념적 명세화

1단계에서는 인공생명기반의 웜 바이러스 모델링 및 시뮬레이션을 위한 목적, 요구사항, 제약사항 등에 대한 개념적 명세화를 통하여 정보통신 기반의 네트워크를 구성한다.

2.2 2단계 : 구조적 및 동역학적 모델 생성

인공생명기반의 웜 바이러스 모델링 및 시뮬레이션을 수행하기 위해서는 인공생명기반의 웜 바이러스에 대한 모델과 인공생명기반의 웜 바이러스가 발현될 수 있는 네트워크에 대한 모델이 필요하다.

인공생명기반의 웜 바이러스의 모델링은 웜 바이러스의 정의와 웜 바이러스가 보이는 인공생명적인 특성에 대한 정의에서부터 시작한다. 웜 바이러스의 정의는 컴퓨터 바이러스가 발전한 종류로 자체 프로그램 코딩을 이용하여 전파되는 자기 복제가 가능한 악성코드이다[2]. 웜 바이러스는 인공생명체로서의 아래의 8가지로 특징을 가진다[3,4].

- 생명의 시공성
- 정보 저장소
- 환경에 반응
- 진화하는 능력
- 자기 복제
- 신진대사
- 안정성 및 복원력
- 성장 및 확장

생명의 시공성 : 생명의 시공성은 인공생명으로서 웜 바이러스가 발현되어 활동하는 동안의 시간과 공간을 의미한다. 따라서 시간적인 특성은 웜 바이러스가 프로세스로서 실행되는 동안의 시간으로 나타낼 수 있다. 공간적인 특성은 웜 바이러스의 수행이 컴퓨터 시스템에서 이루어짐으로 웜 바이러스가 실행되는 컴퓨터 시스템으로 표현할 수 있다.

자기 복제 : 자기 복제는 웜 바이러스가 자체 코드를 이용하여 스스로를 복제하는 악성 프로그램이라는 웜 바이러스의 정의를 통해서 알 수 있다.

정보 저장소 : 정보 저장소는 웜 바이러스가 인공생명

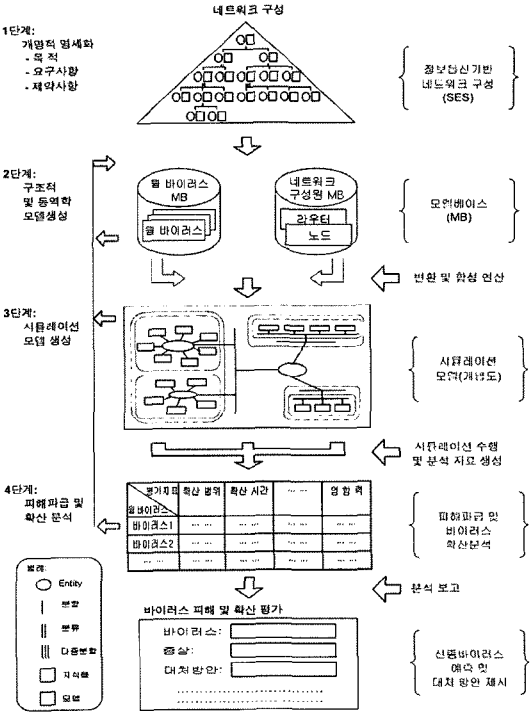


그림 7. 인공생명기반의 웜 바이러스 모델링 및 시뮬레이션을 위한 접근방법

으로써 이전 세대의 유전인자를 다음 세대에 전달하는 과정에서 유전인자의 유전 정보를 저장하는 것을 의미한다.

신진대사 : 신진대사는 생물이 에너지를 사용하여 어떤 행위를 수행하는 것으로 인공생명기반의 웜 바이러스에서는 웜 바이러스가 발현되어 수행되는 것 자체를 의미한다. 컴퓨터시스템에서 웜 바이러스가 실행되는 것은 웜 바이러스가 컴퓨터의 자원을 사용하여 실행되는 것이고 이 과정에서 에너지가 사용되기 때문이다.

환경에 반응 : 환경에 반응은 웜 바이러스의 실행에서 찾을 수 있다. 웜 바이러스는 컴퓨터 시스템에서 사용되는 운영체제와 그 운영체제가 가지는 취약성에 따라서 실행되거나 실행이 중단되기 때문이다. 따라서 인공생명기반의 웜 바이러스는 컴퓨터 시스템의 속성 값에 따라서 생명으로서 발현되거나 죽을 수 있다.

안정성 및 복원력 : 안정성 및 복원력은 인공생명기반의 웜 바이러스가 환경이나 외부의 공격으로부터 생명을 유지하려는 속성이다.

진화하는 능력 : 진화하는 능력은 웜 바이러스의 전파가 E-mail을 이용하는 것을 고려할 때 두 가지로 생각할 수 있다. 첫째는 E-mail에 첨부된 웜 바이러스 코드에 대한 진화이고 둘째는 웜 바이러스 코드를 포함하고 있는 E-mail 본문에 대한 진화이다.

성장 및 확장 : 성장 및 확장은 인공생명체로서의 웜 바이러스의 양적인 증가와 전파를 의미한다. 인공생명기반의 웜 바이러스의 양적인 증가는 웜 바이러스가 실행되는 과정에서 증가되는 메모리와 CPU의 사용량을 통해서 알 수 있고 웜 바이러스의 전파는 웜 바이러스의 정의를 통해서 알 수 있다.

표 1은 웜 바이러스의 인공생명적인 특징이 생물체와 인공생명기반의 웜 바이러스 모델에서 어떻게 반영되는지에 대한 표이다.

네트워크 모델링은 웜 바이러스가 실행되는 컴퓨터 네트워크에 대한 모델링으로 웜 바이러스가 컴퓨터 네트워크에 미치는 영향을 분석하는 역할을 한다. 네트워크 모델은 정보보호 관점에서 바이러스에 대한 시뮬레이션 접근을 위한 보안대책 및 취약성 분석을 위한 필수요소로 인식되고 있다[7]. 따라서 본 논문에서는 인공생명기반의 웜 바이러스 시뮬레이션을 위한 네트워크에 대한 모델링을 위하여 네트워크의 기본요소인 컴퓨터시스템과 라우터에 대한 모델링을 수행하였다.

2.3 3단계 : 시뮬레이션 모델 생성

1단계와 2단계를 통하여 얻은 모델을 사용하여 3단계에서는 인공생명기반의 웜 바이러스 시뮬레이션을 위한 모델을 생성한다.

2.4 4단계 : 피해파급 및 확산 분석

4단계에서는 3단계에서 생성한 시뮬레이션 모델을 사용하여 인공생명기반의 웜 바이러스에 대한 시뮬레이션을 수행하여 인공생명기반의 웜 바이러스에 대한 피해파급 및 확산에 대한 분석을 실행한다.

표 1. 웜 바이러스 모델과 인공생명의 특징

특 징	생 물	웜 바이러스 모델
생명의 시공성	생물이 생명활동을 하는 기간과 공간적인 특성	웜 바이러스 프로세스가 실행되어 종료 될 때까지의 시간과 웜 바이러스가 존재하는 컴퓨터 하드웨어 상의 공간.
환경에의 반응	생물체는 환경의 자극에 반응함	웜 바이러스는 웜 바이러스의 종류에 따라서 실행되는 운영체제가 다름.
자기복제	유전자를 복제하여 자신과 같은 종을 만들어내는 과정	웜 바이러스 프로세스는 E-mail을 통하여 전달됨으로 E-mail을 복사.
안정성과 복원력	다양한 외부 환경에 대하여 생명이 유지될 수 있는 특징	웜 바이러스 프로세서 모델이 활성화되면 이후로 전달되어지는 웜 바이러스 메시지는 프로세스로 되지 못한다.
정보저장소	생명에 관련된 정보를 저장	웜 바이러스를 구분하고 실행할 수 있는 정보를 저장
진화능력	환경의 영향으로 인한 변화	웜 바이러스의 코드가 아닌 데이터 부분에 대한 진화
신진대사	에너지를 소비하는 과정	웜 프로세스의 실행에는 에너지가 필요함
성장과 확장	개체의 물리적 크기 성장	웜 바이러스가 복제한 E-Mail을 다른 컴퓨터 시스템으로 전파

3. 인공생명 기반의 웜 바이러스 시뮬레이션 모델

인공생명기반의 웜 바이러스 모델링의 시뮬레이션을 위한 모델의 전체적인 구조는 그림 2와 같다.

Network 모델 : Network 모델은 웜 바이러스가 발생하는 컴퓨터 네트워크에 해당하는 모델이다.

Net 모델 : Net 모델은 네트워크에서 하나의 Router와 연결된 노드들을 포함하는 단위망을 나타낸다.

Router 모델 : Router 모델은 단위망에 속하는 Router에 대한 모델로 단위망에서 속하는 모든 단말 노드와 연결되어 있다. 그리고 하나의 단위망이 다른 단위망과 연결되어 있다는 것은 각 단위망에 속하는 Router 모델 객체간의 연결이 존재하는 것을 의미한다. Router 모델은 네트워크의 노드에서 생성한 메시지를 전달한다.

Node 모델 : Node 모델은 인공생명기반의 웜 바이러스가 발현되어 활동하는 환경이 되는 컴퓨터 시스템에 대한 모델이다. 인공생명체인 웜 바이러스가 발현되기 위해서는 웜 바이러스가 발현할 수 있는 환경이 조성되어야하기 때문이다. 그림 3는 Node 모델에 대한 구조를 나타낸 것으로 Node 모델은 Network Manager 모델, Scheduler 모델, Processor 모델로 구성된다.

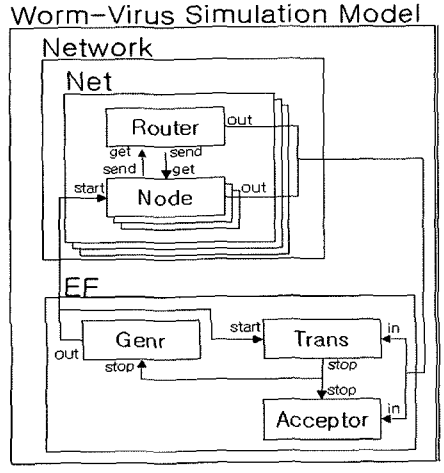


그림 2. 인공생명기반의 웜 바이러스 모델링의 시뮬레이션을 위한 전체구조

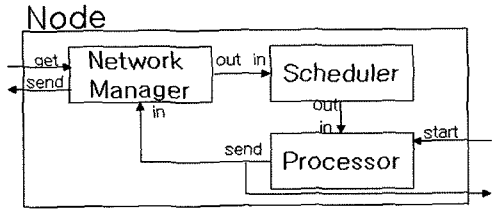


그림 3. Node 모델의 구조

Scheduler 모델 : Scheduler 모델은 Node 모델에 대한 정보를 저장한다. 그리고 Scheduler 모델은 Network Manager 모델에서 받은 인공생명기반의 웜 바이러스를 확인하여 웜 바이러스를 실행하는 Processor 모델에 전달한다.

Network Manager 모델 : 웜 바이러스는 E-mail을 통해서 전파되기 때문에 Network Manager 모델은 Node 모델에 전달된 메시지를 관리하는 모델이다. 표 2는 Network Manager 모델에 대한 의사코드이다. Node 모델은 외부로부터 웜 바이러스가 포함된 E-mail를 받으면 E-mail에서 첨부파일인 웜 바이러스에 해당하는 부분을 Scheduler 모델에 전달한다. 그리고 웜 바이러스를 포함하는 E-mail을 다른 Node모델에 전파하기 위해서 Processor 모델에서 생성한 E-mail를 Router 모델에 전달한다. Network Manager 모델에 전달된 E-mail은 Network Manager 모델이 다른 E-mail을 처리 중이면 E-mail은 버퍼에 싸인다. 이때, 웜

표 2. Network Manager 모델의 의사코드

```
Network Manager
External Transition
    If Phase is 'passive'
        If receive the message on port 'ask'
            Hold-in 'getting'
        If receive the message on port 'in'
            Push the message into the Buffer
    Else
        If Buffer is not full
            Push the message into the Buffer
        else
            Hold-in 'impossible'
Internal Transition
    If Phase is 'checking'
        If the Buffer is empty
            Hold-in 'passive'
        else
            Check the Message
            Hold-in 'getting' or 'sending'
    If Phase is 'sending'
        If the Buffer is empty
            Hold-in 'passive'
        else
            Check the message
            Hold-in 'getting' or 'sending'
Output
    If Phase is 'getting'
        Output: send the message on port 'out'
    If Phase is 'sending'
        Output: send the message on port 'send'
```

바이러스의 공격으로 인해서 버퍼오버플로우가 발생하면 해당 Node의 상태는 'impossible'이 된다. 네트워크에 존재하는 모든 Node의 상태가 'impossible'이 되면 네트워크가 완전히 마비된 것을 나타내고 시뮬레이션을 종료한다.

Processor 모델 : 컴퓨터시스템이 웜 바이러스에 감염되었다는 것은 웜 바이러스 프로그램이 실행되었다는 것을 의미한다. 따라서 인공생명 기반의 웜 바이러스 모델은 인공생명기반의 웜 바이러스가 생명체로서 발현하여 생명활동을 하는 것을 표현하기 위해서 Processor 모델을 사용한다. Processor 모델은 그림 4와 같이 Identifier 모델, Duplicator 모델, Propagator 모델로 구성된다.

Identifier 모델 : 인공생명기반의 웜 바이러스가 생명으로서 발현되기 위해서는 인공생명기반의 웜 바이러스의 환경인 Node 모델에 대한 정보를 확인하여야 한다. Identifier 모델은 이러한 과정을 위하여 Node 모델의 특성을 확인하는 모델이다. 표 3은 Identifier 모델의 의사결정 코드이다.

Duplicator 모델 : Duplicator 모델은 인공생명체인 웜 바이러스의 유전인자인 E-mail를 복제하여 다음 세대에 전달하는 과정을 수행하는 모델이다. 본 논문에서 E-mail을 인공생명기반의 웜 바이러스의 유전인자로 인식하는 이유는 인공생명체인 웜 바이러스가 E-mail를 사용하여 자신의 코드를 다음 세대의 웜 바이러스에 전달하기 때문이다. 유전인자를 전달하는 과정에서는 모든 유전인자가 변화 없이 전해지는 자기 복제 과정과 일부의 유전인자의 변형이 일어나는 진화가 있다. 따라서 Duplicator 모델은 자기 복제와 진화의 과정을 수행한다. 표 4는 Duplicator 모델에 대한 의사결정 코드이다.

Propagator 모델 : Duplicator 모델에서 생성된 E-mail을 전파하기 위해 E-mail의 Target에 대한 IP주소를 Random 함수를 이용하여 생성하는 모델이다. Propagator 모델은 E-mail의 Target IP를 생성한 뒤 Node 모델의 Network Manager 모델로 E-mail를 전달한다. 표 5는 Propagator 모델의 의사코드이다.

EF 모델 : 인공생명기반의 웜 바이러스 모델을 이용하여 시뮬레이션을 하기 위해 필요한 모델로 시뮬레이션의 시작과 종료, 결과 분석을 위한 Gern 모델, Trans 모델, Acceptor 모델로 구성된다.

Gern 모델 : 시뮬레이션의 초기에 웜 바이러스를 포함하는 E-메일을 네트워크의 한 Node에 전달하는 역할을 수행한다.

Trans 모델 : Trans 모델은 시뮬레이션이 종료조건을

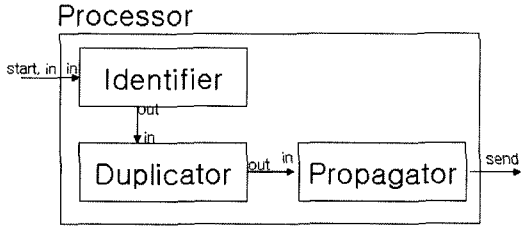


그림 4. Processor 모델의 구조

표 3. Identifier 모델의 의사코드

```
Identifier
External Transition
    If Phase is 'passive'
        If receive message on port 'start'
            Hold-in 'checking'
    Else
        Keep the state
Internal Transition
    If Phase is 'checking'
        Hold-in 'passive'
Output
    If Phase is 'checking'
        If processing condition is fired
            Output: send the Message on port 'out'
```

표 4. Duplicator 모델의 의사 코드

```
Duplicator
External Transition
    If Phase is 'passive'
        If receive Message on port 'in'
            Hold-in 'creating'
Internal Transition
    If Phase is 'creating'
        Hold-in 'creating'
Output
    If Phase is 'creating'
    Output: Send the Message to port 'out'
```

표 5. Propagator 모델의 의사 코드

```
Propagator
External Transition
    if Phase is 'passive'
        If receive value on port 'in'
            Hold-in 'waiting'
Internal Transition
    If Phase is 'waiting'
        Hold-in 'passive'
Output
    If Phase is 'waiting'
    Output : Send the Message to port 'out'
```

검사하는 모델이다. Trans 모델은 웜 바이러스에 의해서 네트워크가 마비되거나 정의된 시간이 되면 시뮬레이션의 종료조건이 만족한 것으로 판단하여 인공생명기반의 웜 바이러스에 대한 시뮬레이션을 종료 시킨다.

Accrptor 모델 : 시뮬레이션을 종료하는 메시지를 받고 시뮬레이션의 결과를 분석한다.

4. Case Study

인공생명기반의 웜 바이러스 시뮬레이션은 인공생명기반의 웜 바이러스 모델링과 네트워크 모델링을 통하여 얻어진 모델을 통하여 수행된다.

4.1 인공생명 기반의 웜 바이러스 모델링

인공생명기반의 웜 바이러스 시뮬레이션은 I-worm 계열의 MyDoom 웜 바이러스 모델을 기반으로 수행하였다[8][9]. MyDoom 웜 바이러스는 웜 바이러스의 코드를 E-mail의 첨부파일로 전달하는 웜 바이러스로 E-mail를 생성할 때, E-mail의 제목과 본문의 내용을 임의의 문자열로 생성한다. 표 6은 MyDoom 웜 바이러스를 기반으로 모델링한 인공생명기반의 웜 바이러스 시뮬레이션을 위한 웜 바이러스 모델의 구조를 나타낸다.

4.2 네트워크 모델링

인공생명기반의 웜 바이러스 시뮬레이션을 수행한 네트워크 모델은 1997년 IEEE에 발표된 "Modeling the Global Inter"에서 사용된 네트워크의 기본 단위의 네트워크 모델을 채택하였다[10]. 표 7은 "Modeling the Global Internet"의 기본 네트워크를 모델링하여 얻은 인공생명기반의 웜 바이러스 시뮬레이션을 위한 초기조건을 나타내고 그림 5는 인공생명기반의 웜 바이러스 시뮬레이션을 수행한 네트워크에 속한 Router 모델에 대한 연결을 나타낸다.

표 6. 인공생명기반의 웜 바이러스 모델 구조

Attributes	Value
Source IP	200.200.200.1
Target IP	200.200.100.1
Sender	"Test"
Title	"Hello"
Body	"I love you"
웜 바이러스 정보	"Slammer"

표 7. 인공생명 기반의 웜 바이러스 시뮬레이션 초기조건

모 델		객체수
Net 모델		100개
Router 모델	OSFP With LAN	71개
	OSFP Without LAN	29개
Node 모델		710개

4.3 인공생명기반의 웜 바이러스 시뮬레이션 결과

인공생명기반의 웜 바이러스 시뮬레이션은 인공생명기반의 웜 바이러스의 전파, 환경에 반응, 진화에 대하여 수행하였다.

4.3.1 인공생명기반의 웜 바이러스 전파

인공생명기반의 웜 바이러스의 전파에 대한 시뮬레이션은 인공생명으로서 웜 바이러스가 보이는 성장 및 전파에 대한 시뮬레이션 결과로 인공생명기반의 웜 바이러스 모델과 웜 바이러스와의 전파에 대한 성질을 비교하기 위하여 시뮬레이션 실험이다. 인공생명기반의 웜 바이러스 전파실험의 결과는 그림 6과 같다. 인공생명기반의 웜 바

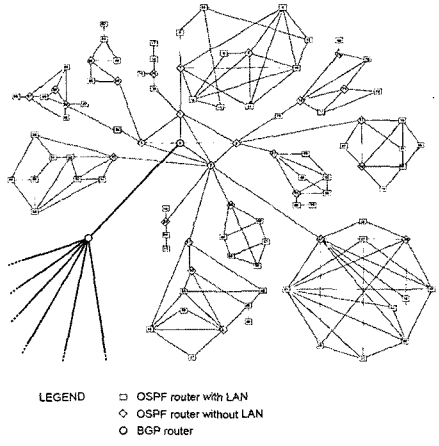


그림 5. Router 모델의 연결도

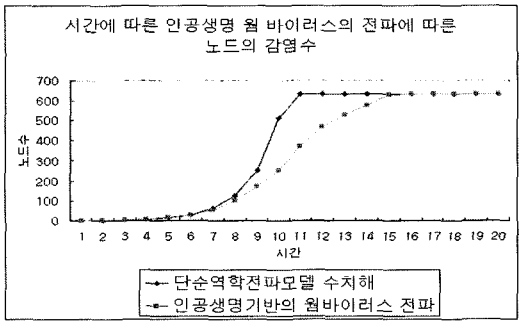


그림 6. 인공생명기반의 웜 바이러스 전파

이러스의 전파를 나타내는 그래프는 초기에는 작은 증가를 보이다 급격한 증가를 보이고 일정 시간이 지난 후 수렴하는 단순역학전파 모델의 수치해를 통하여 얻은 그래프의 변화와 같은 패턴을 보인다. 수치해의 그래프와 인공생명기반의 웜 바이러스 시뮬레이션 실험의 결과가 차이를 보이는 것은 시뮬레이션 실험에서는 수치해의 식에서 고려되지 않은 Router 모델에 의한 지연현상이 나타났기 때문이다.

4.3.2 발현 환경에 따른 인공생명기반의 웜 바이러스 발현

발현 환경에 따른 인공생명기반의 웜 바이러스발현에 대한 시뮬레이션을 수행하기 위해서 네트워크 모델은 윈도우즈 시스템과 리눅스 시스템으로 구성되어있으며 모든 Node 모델은 E-mail 프로그램을 실행할 수 있다고 가정한다. 또한, 각각의 Node 모델 객체는 특정한 웜 바이러스의 공격에 대하여 취약성이 존재하는 객체와 존재하지 않는 객체로 구분된다. 그림 7은 이러한 가정을 4.1에서 모델링한 인공생명기반의 웜 바이러스의 시뮬레이션의 발현 환경으로 설정하였을 때 발현 환경에 따른 인공생명기반의 웜 바이러스 발현에 대한 시뮬레이션 실험에 대한 결과이다. 인공생명기반의 웜 바이러스 시뮬레이션을 수행한 웜 바이러스는 Windows시스템에서 실행되는 웜 바이러스로 시뮬레이션 결과 Windows시스템이면서 취약성이 존재하는 Node 모델에서만 발현되었다.

4.3.3 인공생명기반의 웜 바이러스 진화

본 논문에서 인공생명기반의 웜 바이러스의 시뮬레이션을 수행하기 위해서 모델링한 MyDoom 웜 바이러스는 E-mail을 생성할 때 마다 E-mail 의 Title과 Body에 해당하는 값을 임의로 생성한다. 따라서 인공생명기반의 웜 바이러스 진화 실험의 결과는 그림 8과 같이 생성될 때마다 다른 Title 값과 Boby의 내용을 포함한다.

인공생명기반의 웜 바이러스 모델링 및 시뮬레이션을 통하여 웜 바이러스가 가지는 전파, 환경에 반응, 진화에 대한 인공생명적인 특성을 시뮬레이션을 통하여 확인하였다.

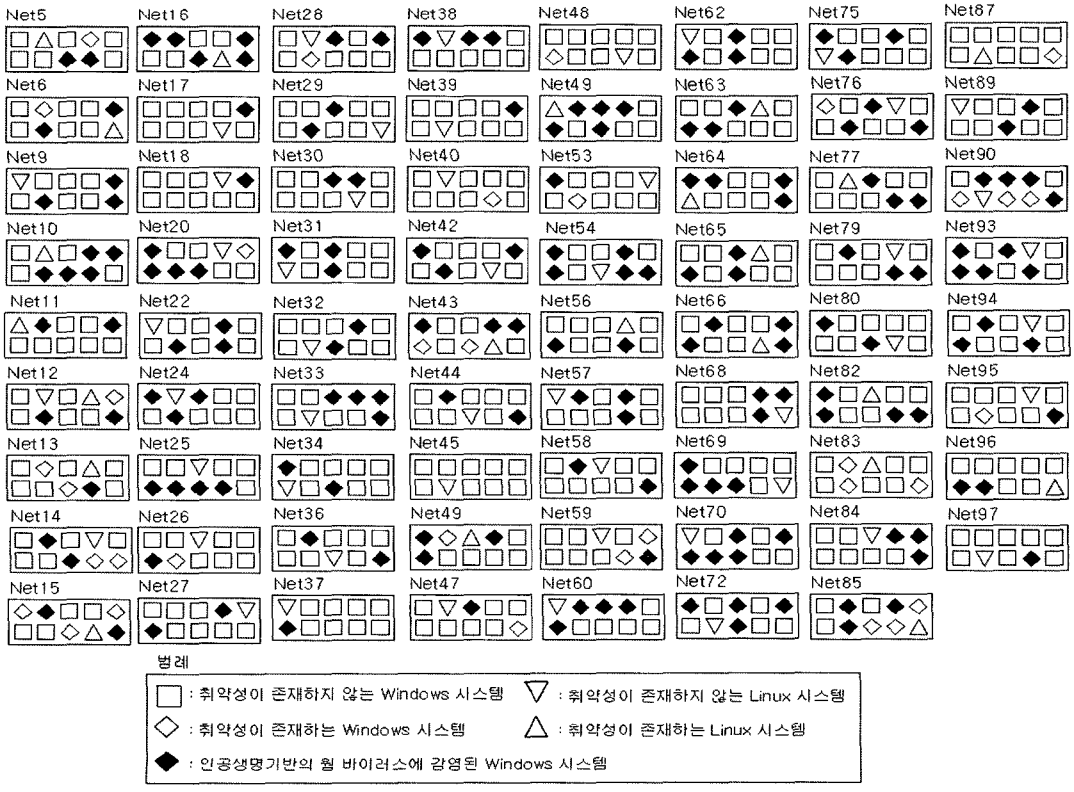


그림 7. 환경에 따른 인공생명기반의 웜 바이러스 발현

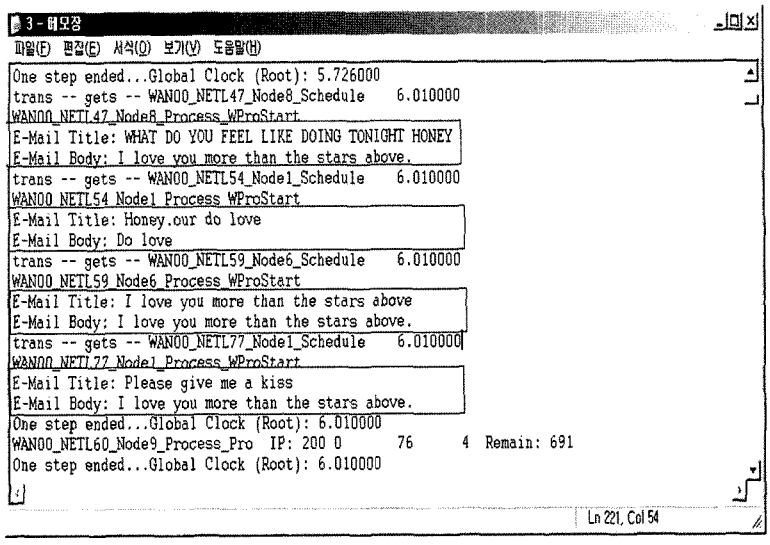


그림 8. 인공생명기반의 웜 바이러스의 진화

5. 결 론

기존에 컴퓨터 바이러스 모델링에 관한 연구는 컴퓨터 바이러스자체에 대한 연구 보다는 네트워크에 관한 연구가 주를 이루었다. 하지만 본 논문에서는 인공생명의 관점에서 웜 바이러스에 대해 모델링함으로써 웜 바이러스가 나타내는 인공생명체적인 특성까지 모델링의 범주에 포함할 수 있다. 따라서 향후 연구로는 본 논문에서 제시한 모델링 및 시뮬레이션 방법을 기반으로 실제 웜 바이러스의 전파 경로, 위험 파급 효과 등의 여러 가지 실험이 진행되어야 한다. 또한, 이를 기반으로 웜 바이러스가 네트워크에 미치는 영향뿐 아니라 웜 바이러스의 탐지 방법에 대한 연구에 활용할 수 있을 것으로 기대된다. 또한 웜 바이러스의 동작 메커니즘에 대한 분석도 가능하게 되어 컴퓨터 바이러스 백신 연구에도 기여할 것으로 기대된다.

6. 향후 연구

본 논문은 인공생명기반의 웜 바이러스에 대한 모델을 제시하였다. 따라서 향후 연구로는 본 논문에서 제시한 인공생명기반의 모델을 사용한 시뮬레이션을 수행함으로써 얻은 웜 바이러스의 예측이나 대처방안이 실제 네트워크에서 실행되는 웜 바이러스에 대한 예측이나 대처방안으로 사용되었을 경우 같은 결과를 나타내는 지에 대한 연구가 이루어져야 한다.

Acknowledgement

본 논문은 과학기술부 한국과학재단 지정 경기도 지역협력 연구센터(RRC)인 한국항공대학교 인터넷 정보검색 연구센터(IRC)의 지원에 의한 것임.

참 고 문 헌

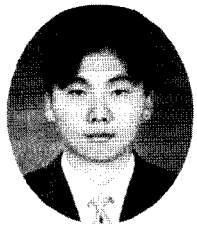
1. T.A Longstaff, C.Chittister, R.Pethia, Y.Y. Haimes (2000), "Are We Forgetting the Risks of Information Technology", IEEE Computer.
2. Grimes, Roger A. (2001), "Malicious Mobile Code", O'REILLY.
3. Eugene H Spafford (1994), "Computer Viruses as Artificial Life", Journal of Artificial Life, MIT Press.
4. Eugene H, Spafford (1991), "Computer Viruses, A Form of Artificial Life", Technical Report CSD-TR-985, Purdue University.
5. 한국정보보호진흥원, http://www.kisa.or.kr.
6. 유용준, 이장세, 지승도 (2004), "SIMVA를 이용한 시뮬레이션 기반의 네트워크 취약성 분석", 한국시뮬레이션학회 논문지, 13권 3호, pp. 21-29.
7. 이철원, 김홍근 (2000), "정보보증:컴퓨터보안의 새로운 패러다임", 정보과학회지, 제18권 제1호, pp. 53-61.
8. 안철수연구소, http://www.Anlab.com.
9. 하우리, http://www.hauri.co.kr/virus/virus info/virussearch_ read.html.
10. J. Cowie, D. Nicol, and A. Ogielski (1999), "Modeling

the Global Internet", IEEE Computing in Science & Engineering.
11. Fred Cohen (1999), "simulating Cyber Attacks Defenses, and Consequences". 1999 IEEE Symposium on Security and Privacy Special 20th Anniversary Program, The Claremont Resort Berkeley, California.
12. Amoroso, E. (1999), Intrusion Detection, AT&T Laboratory, Intrusion Net Books, January.
13. Nong Ye, Joseph Giordano, CACS - A Process Control Approach to Cyber Attack Detection, Communications of the ACM..
14. B.P, Zeigler (1990), Object-oriented Simulation with Hierarchical, Modular Models: Intelligent Agents and Endomorphic systems, Academic Press, San Diego, CA.[11].
15. B.P, Zeigler, Kim, T.G. and Praehofer (1990), H. Theory of Modeling and Simulation. 2ed. Academic Press, New York, NY.
16. Chi, S.D (1991), Modeling and Simulation for High Autonomy Systems, Ph.D. Dissertation, Dept. of Electrical and Computer Engineering, Univ. of Arizona.
17. Carey Nachenberg, "Computer Parasito- logy", http://www.virusbtn.com, Symantec AntiVirus Rearch Center.

오 지 연 (hyndong@empal.com)

2004년 한국항공대학교 컴퓨터공학과 학사
2006년 한국항공대학교 컴퓨터공학과 석사
2005년~현재 (주)챈스아이 근무

관심분야 : 인공지능



유 용 준 (ilog21c@hau.ac.k)

2003년 한국항공대학교 컴퓨터공학과 학사
2005년 한국항공대학교 컴퓨터공학과 석사
2005년~현재 한국항공대학교 컴퓨터공학과 박사 과정

관심분야 : 모델링 및 시뮬레이션, 네트워크 보안

채 수 환 (chae@hau.ac.kr)

1973년 한국항공대학교 항공전자 공학과 학사
1985년 미국 Univ. of Alabama 전산공학과 석사
1985년 미국 Univ. of Alabama 전기공학과 박사
1977년~1983년 금성통신 연구원 근무
1989년~현재 한국항공대학교 항공전자 및 정보통신공학부 교수

관심분야 : 컴퓨터구조, 병렬처리시스템

지 승 도 (sdchi@hau.ac.kr)

1982년 연세대학교 전기공학과 학사
1984년 연세대학교 전기공학과 석사
1985년~1986년 두산 컴퓨터 (현 한국 디지틸) 근무
1991년 미국 아리조나대학교 전기전산공학과 박사
1992년 미국 SIMEX Systems and S/W 회사 S/W 담당자로 근무
1992년~현재 한국항공대학교 항공전자 및 정보통신공학부 교수

관심분야 : 이산사건 시스템 모델링 및 시뮬레이션, 컴퓨터 보안, 지능시스템 디자인 방법론, 시뮬레이션 기반 인공생명, 교통 모델링