

패킷 네트워크를 이용한 네트워크 모델링 시뮬레이션¹⁾

김정식[○] 조재익 최경호 박진호 권원홍 임을규
한양대학교 정보통신대학

{bisa1004[○], whisperj}@hanmail.net, ckh820520@naver.com, pjh0347@yahoo.co.kr,

whkwon@enc.hanyang.ac.kr, imeg@hanyang.ac.kr

Network Modeling Simulation using Packet networks

Jung Sik KIM[○], Jae Ik Cho, Kyoung Ho Choi, Jin Ho Park, Wonhong Kwon, Eul Gyu IM
College of Information Communications, Hanyang Univ.

요 약

인터넷 보급에 따라 웬에 의한 피해가 꾸준히 이어지고 있다. 인터넷 웬을 방어하기 위해서는 웬에 대한 연구가 이루어져야 하는데 웬을 연구하기 위해 대규모 네트워크를 구성하여 연구하기에는 어려움이 따르게 된다. 그래서 실제 네트워크를 구성하는 대신 시뮬레이션을 이용한 연구가 이루어지게 되었는데 시뮬레이션이라 할지라도 대규모 네트워크를 시뮬레이션 하는 것은 여러 문제점이 존재하게 된다. 그래서 본 논문에서는 대규모 네트워크를 시뮬레이션 하기 위해 네트워크 모델링 시뮬레이션 방법을 기본으로 한 패킷 네트워크를 이용한 네트워크 모델링 시뮬레이션 방법에 대해 제안을 하였다. 이 방법을 기존의 대규모 네트워크 시뮬레이션의 문제를 패킷 네트워크와 모델링 네트워크가 서로 보완을 하여 해결하도록 구성되어 있다. 그리고 제안한 방법을 이용하여 웬의 전파를 실험한 시뮬레이션을 수행해 보았다.

1. 서 론

인터넷이 널리 보급되면서 그에 비례하여 인터넷 웬에 대한 피해도 같이 증가하게 되었다. 이에 인터넷 웬을 방어하기 위해서 여러 가지 연구가 진행되고 있는 상황이다. 하지만 인터넷 웬에 대한 연구를 하기 위해서는 여러 가지 제약 조건들이 있게 되는데 그 중 하나는 웬을 실험하는 환경을 구축하는데 어려움이 따른다는 것이다. 일례로 slammer worm의 경우에는 최소 7만 5천 호스트 이상이 감염되었다고 하는데^[1] 이 웬을 연구하기 위해서 수 만개의 노드로 구성된 네트워크를 구축하기란 불가능에 가깝다. 그래서 이렇게 대규모의 네트워크가 필요한 연구를 수행하기 위해서 네트워크 시뮬레이션을 이용한 방법이 많이 사용되고 있다.

네트워크 시뮬레이션을 사용하는 것이 실제 네트워크를 구축하는 것보다 훨씬 효율적이지만 시뮬레이션을 이용한 방법도 수만~수십만 노드로 구성되는 대규모 네트워크를 시뮬레이션 하기에 어려움이 따른다. 네트워크 시뮬레이션을 수행하게 되면 시뮬레이터가 네트워크에 존재하는 각 노드들을 가상으로 설정을 하여 관리를 하고, 패킷의 전송, 손실 등 네트워크에서 발생하는 이벤트들도 모두 일일이 처리를 해주게 된다. 이 때 네트워크의 노드 수가 증가하면 할수록 그에 비례하여 시뮬레이션 이벤트의 발생량도 증가하기 때문에 결과적으로 전체 시뮬레이션 수행 시간은 매우 가파르게 증가하게 된다.

이런 이유로 대규모 네트워크의 시뮬레이션을 한번 수

행하게 되면 그 수행 시간이 수십 시간 이상이 걸리게 된다. 시뮬레이션 수행 시간도 줄이고 시뮬레이션을 좀 더 효율적으로 수행하기 위해서 네트워크를 모델링 하여 모델링 네트워크를 시뮬레이션 하는 방법도 사용하게 된다. 네트워크 모델링 시뮬레이션은 수행시간의 측면에서는 기존의 대규모 네트워크 시뮬레이션을 그대로 수행하는 것보다 큰 이점을 가지고 있지만, 네트워크 현상을 특정 모델에 적용하면서 많은 부분을 단순화, 추상화 시켰기 때문에 시뮬레이션에 실제 네트워크 현상을 제대로 반영하지 못하는 문제가 생기게 되었다.

그래서 본 논문에서는 대규모 네트워크 시뮬레이션과 네트워크 모델링 시뮬레이션에서 발생하는 문제를 해결할 수 있는 방안으로 패킷 네트워크라 명하는 소규모 네트워크 시뮬레이션을 이용한 네트워크 모델링 시뮬레이션 방법을 제안하였다.

본 논문 2장에서는 위에서 언급한 대규모 네트워크 시뮬레이션 및 네트워크 모델링 시뮬레이션의 문제점에 대해서 자세히 살펴보고, 3장에서는 패킷 네트워크를 이용한 네트워크 모델링 시뮬레이션 방법을 제안하였다. 4장에서는 제안한 방법을 이용하여 실제로 네트워크 시뮬레이션을 수행한 실험 결과에 대해 말하고, 마지막으로 결론을 내리게 된다.

2. 대규모 네트워크 시뮬레이션 및 네트워크 모델링 시뮬레이션의 문제

실제 네트워크를 기반으로 네트워크 시뮬레이션을 수행하게 되면 시뮬레이션 네트워크의 추상화 정도를 선택해야 한다. 전체 네트워크 중에서 필요 없는 노드를 제외해야 하는지, 수행 시간 단위는 실제 시간대와 맞추어

1) 본 연구는 국가보안기술연구소의 지원으로 수행되었음.

야 하는 저 등 시뮬레이션 네트워크를 구성하기 위해 선택을 해야 한다.

대규모 네트워크 시뮬레이션은 규모가 크지만 실제 네트워크와 비슷한 네트워크를 구성하여 네트워크 현상을 비교적 자세히 알거나, 특정 현상을 관찰하고 싶을 때 선택하여 사용할 수 있다. 반대로 네트워크 모델링 시뮬레이션은 복잡한 네트워크를 단순화 시켜 빠르고 효과적으로 시뮬레이션을 수행하여 네트워크 현상의 흐름을 쉽게 파악할 수 있도록 해준다. 이런 장점에도 불구하고 대규모 네트워크 시뮬레이션과 네트워크 모델링 시뮬레이션 중 하나만을 선택하기에는 문제가 있다. 이 장에서는 이 두 가지 시뮬레이션 방법의 문제에 대해서 살펴본다.

2.1 대규모 네트워크 시뮬레이션의 문제

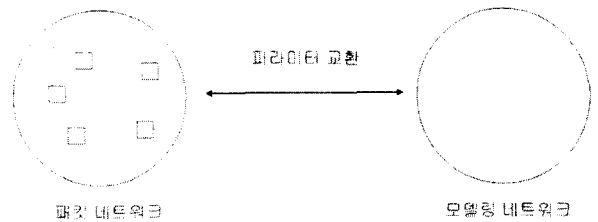
가장 단순하게 대규모 네트워크 시뮬레이션을 수행하는 방법은 실제 네트워크 또는 비슷한 구조의 네트워크를 기반으로 하여 시뮬레이션 네트워크를 구성한 뒤 시뮬레이션을 수행하는 것이다. 이 방법은 네트워크의 노드들이 독립적으로 동작하기 때문에 특정 노드의 동작을 확인하기 쉽고, 패킷 수준의 네트워크 관찰과 같이 시뮬레이션 네트워크를 자세하게 파악할 수 있다는 장점이 있다. 하지만 대규모 네트워크 시뮬레이션을 수행하기에는 큰 문제점이 따르는데 가장 큰 문제는 네트워크의 구성 및 수행 시간의 문제이다.

시뮬레이션을 위해 소규모의 시뮬레이션 네트워크를 구성하는 경우, 네트워크 노드의 수도 적고, 그 연결망도 그리 복잡하지 않기 때문에 네트워크의 구조를 미리 구상해 두었다면 그리 어렵지 않게 시뮬레이션 네트워크를 구성할 수 있다. 하지만 시뮬레이션 네트워크를 구성하는 노드의 수가 수 만개 이상 증가하게 되면 이를 생성하고 연결을 해주는 일 자체만 해도 큰 어려움이 따르고, 네트워크 연결을 위한 토폴로지 구상도 힘든 작업이 된다.

대규모 네트워크 시뮬레이션을 위한 시뮬레이션 네트워크를 구성하였다 하여도, 시뮬레이터가 관리해야 하는 네트워크 노드도 많고, 시뮬레이션에서 발생하는 이벤트의 수도 노드의 수에 비례하여 발생하게 된다. 실제로 4장의 실험에서 사용하는 200노드의 소규모 네트워크를 100초간 시뮬레이션 하였을 경우 약 15만개 정도의 이벤트가 발생하였다. 그러므로 수만 노드 이상의 대규모 네트워크를 시뮬레이션 하게 되면 노드의 수에 비례하여 발생하는 이벤트의 수도 급격히 증가하게 된다. 이는 시뮬레이션 수행 시간의 증가로 이어지게 된다.

2.2 네트워크 모델링 시뮬레이션의 문제

네트워크 시뮬레이션을 수행 하는 방법에는 시뮬레이션을 원하는 네트워크를 수학적으로 계산된 특정 모델에 맞추어 구성을 하여 이렇게 구성된 모델링 네트워크를 이용하여 시뮬레이션을 수행하는 네트워크 모델링 시뮬레이션 방법이다. 네트워크 모델링 시뮬레이션은 대규모 네트워크를 시뮬레이션 할 경우 발생하는 네트워크



[그림 1] 시뮬레이션 네트워크 구조

구성과 수행시간의 문제점을 해결할 수 있는데 이는 네트워크 모델을 사용하기 때문이다. 모델링 네트워크를 사용하면 대규모 네트워크라 하여도 선택된 모델에서 원하는 구조에 맞추어 간단한 네트워크를 구성하면 되기 때문에 네트워크 구성을 하기 위한 어려움이 줄어들게 되고, 대부분 수학적인 계산을 통해 시뮬레이션을 수행하기 때문에 시뮬레이션 수행 시간도 급격히 감소하게 된다. 하지만 이 방법은 대규모 네트워크 시뮬레이션의 단점을 해결하였지만 대규모 네트워크 시뮬레이션의 장점인 부분이 문제가 된다. 우선 특정 모델에 네트워크를 맞추어 구성을 하기 위해서는 실제 네트워크의 많은 정보를 잃어버리게 된다. 그래서 시뮬레이션 네트워크의 전체적인 현상을 관찰하기에는 유리하지만 노드 또는 패킷별로 자세한 관찰을 수행하기는 힘들다. 또 시뮬레이션이 수행되는 중간에 특정 네트워크 현상이 발생하였다 하더라도 이를 모델링 네트워크에 동적으로 반영하기 힘들다는 단점이 있다. 갑작스런 노드의 추가 혹은 비정상적인 패킷 발생량의 증가와 같이 모델을 설계하면서 미리 계획하지 않은 부분에 대해서는 시뮬레이터가 효과적으로 대처할 수 없는 것이다.

3. 패킷 네트워크를 이용한 네트워크 모델링 시뮬레이션

3.1 개요

대규모 네트워크 시뮬레이션 방법과 네트워크 모델링 시뮬레이션 방법은 각각 문제점을 가지고 있다. 이 장에서는 네트워크 모델링 시뮬레이션을 기반으로^{[2][3]} 하여 이 방법의 단점을 보완할 수 있도록 해주는 패킷 네트워크를 사용하는 방법에 대해 제안한다.

패킷 네트워크는 네트워크 모델링 시뮬레이션의 문제점인 노드 단위의 관찰 및 네트워크 현상의 동적인 움직임을 표현해 주기 위해 모델링 네트워크와 연결된 소규모 네트워크를 뜻한다. 그림 1은 패킷 네트워크와 모델링 네트워크로 구성된 가장 간단한 구조의 시뮬레이션 네트워크의 구조이다.

패킷 네트워크에서 네트워크 현상 및 특정 이벤트가 발생하면 이 정보를 파라미터를 통해 모델링 네트워크에 전달해 주게 된다. 그러면 모델링 네트워크는 이 정보를 사용하여 현재 시뮬레이션을 동적으로 업데이트하게 된다.

또한 시뮬레이션 수행 중 특정 노드 및 패킷을 관찰하

고 싶을 때는 패킷 네트워크에 존재하는 노드 및 패킷을 찾아 관찰하게 된다.

이장의 남은 부분은 패킷 네트워크와 모델링 네트워크에 대해 세부적인 내용을 설명하고 이 두 네트워크 사이에 파라미터를 교환하는 방법에 대해 설명을 하였다.

3.2 패킷 네트워크

패킷 네트워크는 모델링 네트워크와 연결되어 있는 소규모 네트워크이다. 패킷 네트워크는 대규모 네트워크 시뮬레이션에서 대규모 네트워크가 가지는 장점을 적용하기 위해 구성된 네트워크로, 네트워크의 규모는 작지만 자세하게 구성되어 네트워크를 관찰하기 쉽게 구성된다. 또한 실제 네트워크에서 발생하는 특별한 이벤트를 표현할 수 있기 때문에 이를 이용하여 모델링 네트워크에 적용할 수 있게 된다.

패킷 네트워크는 네트워크 모델링 시뮬레이션에서 동적으로 업데이트 해주기 위한 정보들을 수집하고, 정리하여 모델링 네트워크로 전달하는 역할을 한다. 적절한 정보를 수집하기 위해서 패킷 네트워크의 규모는 시뮬레이션 상황에 따라 다르게 되는데 패킷 네트워크를 사용하는 목적인 수행 시간의 감소를 위해서 적당한 수준의 노드 수를 선택해야 할 것이다. 덧붙여 시뮬레이션 시나리오를 정확히 이해하고 있다면 패킷 네트워크의 시뮬레이션 수준도 그에 맞추어 적절한 수준을 선택하게 한다.

3.3 모델링 네트워크

모델링 네트워크는 네트워크 모델링 시뮬레이션을 수행하기 위한 시뮬레이션 네트워크이다. 제안하는 시뮬레이션 방법이 네트워크 모델링 시뮬레이션을 기반으로 하기 때문에 모델링 네트워크는 기존의 네트워크와 비교하여 크게 변화되는 점은 없게 된다. 하지만 동적인 네트워크 환경을 표현해 주기 위해서 패킷 네트워크에서 수집되어 보내지는 정보를 이용하여 모델링 네트워크의 파라미터들을 수정, 반영해 주는 기능이 추가되어야 한다. 그러기 위해서는 모델링 네트워크를 구성하는 단계에서 패킷 네트워크와의 연동이 가능한지를 고려하여 네트워크를 구성하여야 한다.

3.4 파라미터 교환

네트워크 모델링 시뮬레이션을 동적으로 업데이트하기 위해서는 패킷 네트워크와 모델링 네트워크 사이에 네트워크 파라미터 교환이 이루어 져야한다. 파라미터의 전달은 주로 패킷 네트워크에서 모델링 네트워크로 전달되게 된다. 하지만 모델링 네트워크의 파라미터를 패킷 네트워크에 전달해야 하는 상황이 발생한다면 모델링 네트워크에서 패킷 네트워크로의 파라미터 전달도 이루어 지게 된다.

네트워크 간의 파라미터 전달을 위해 가장 중요한 것은 어느 파라미터를 전달하느냐의 문제이다. 웜의 시뮬레이션을 수행하는 상황일 때 패킷 네트워크에서는 노드

의 감염률, 치료율, 웜에 의한 네트워크 트래픽의 증가율, 전체 패킷의 손실률과 같은 정보를 수집할 수 있다. 시뮬레이터의 한 종류인 SSFNet^[4]에서 'Code-Red Worm v2'을 EPIDEMIC 모델을 통해 구현을 하였는데^{[4],[5]} 이 모델링 네트워크에서 시뮬레이션을 위해 사용되는 파라미터 중 하나가 웜의 감염률이다. 이 경우 패킷 네트워크에서 수집되어 전달되어야 하는 파라미터 중 하나는 이 웜의 감염률이 되어야 할 것이다.

파라미터를 교환하기 위해서 해결해야 하는 다른 문제는 두 네트워크 사이의 시뮬레이션 시간 동기화의 문제이다. 기본적으로 패킷 네트워크와 모델링 네트워크는 시뮬레이션 성격이 다르기 때문에 시뮬레이션 시간대가 다르다. 또, 패킷 네트워크의 경우에는 짧은 시간단위로 시뮬레이션이 동작을 하게 되는데 모델링 네트워크는 이에 비해 긴 시간단위로 시뮬레이션이 동작하게 된다. 그렇기 때문에 패킷 네트워크에서 수집된 파라미터를 모델링 네트워크에 전달해 주기 위해서는 두 네트워크 사이의 시간 동기화가 필요하게 된다.

4. 실험

본 논문에서 제안한 방법을 이용하여 웜의 전파에 대한 간단한 시뮬레이션을 수행해 보았다. 시뮬레이터는 SSFNet을 사용하였는데 시뮬레이션 환경에 대한 내용은 표 1에 나와 있다.

CPU	Intel 3.0 GHz
RAM	1GB RAM
OS	Debian GNU/Linux
Simulator	SSFNet 2.0

[표 1] 시뮬레이션 환경

4.1 시뮬레이션 대상

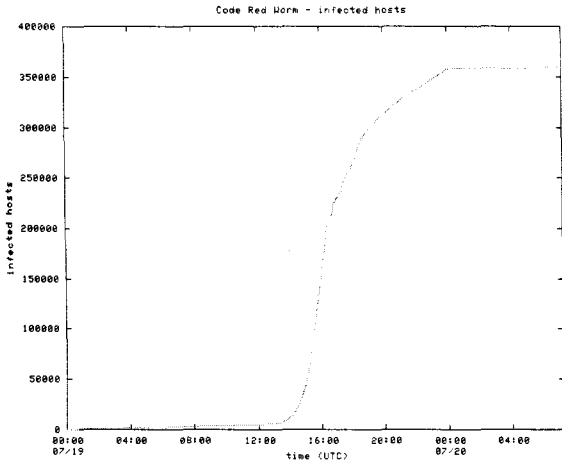
이 시뮬레이션에서는 'Code-Red Worm v2'과 유사한 형태로 전파되는 웜을 시뮬레이션 하였다.

패킷 네트워크의 호스트는 정상적일 경우 임의의 크기 패킷을 생성하여 전송하게 되는데 특정 호스트가 웜에 감염되게 되면 그 호스트는 4KB의 패킷을 생성하여 네트워크에 뿌리게 된다.

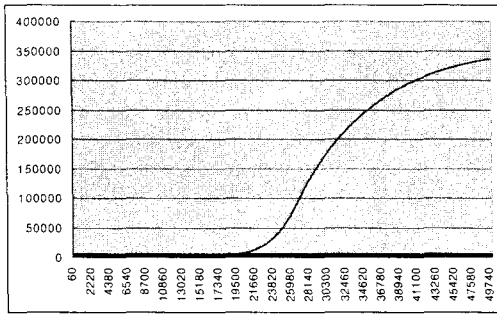
모델링 네트워크는 epidemic 모델을 이용하여 시뮬레이션을 수행하게 되는데 패킷 네트워크에서 모델링 네트워크로 전달되는 파라미터는 웜의 감염 비율이다. 모델링 네트워크에서는 패킷 네트워크에서 전달된 감염률을 이용하여 대규모 호스트에서 웜의 전파를 시뮬레이션하게 된다.

4.2 네트워크 구성

전체 시뮬레이션 네트워크 구성은 패킷 네트워크 1개와 모델링 네트워크 1개로 구성되어 있다. 패킷 네트워크는 200노드의 호스트로 구성되어 있고, 네트워크를 구



[그림 2] Code Red v2의 실제 전파 그래프



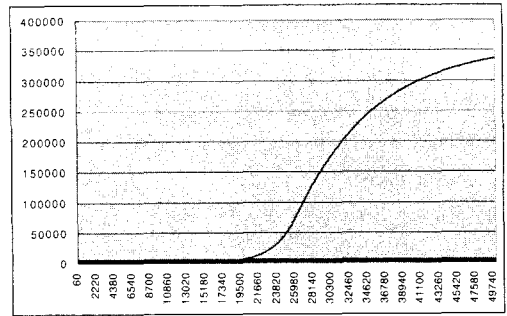
[그림 3] Code-Red v2 모델링 시뮬레이션

성하기 위해 약 30개의 라우터가 존재한다. 모델링 네트워크는 epidemic 모델을 이용한 전파 모델을 사용하는데 모델링 네트워크 안의 호스트의 수는 36만개로 설정되어 있다.

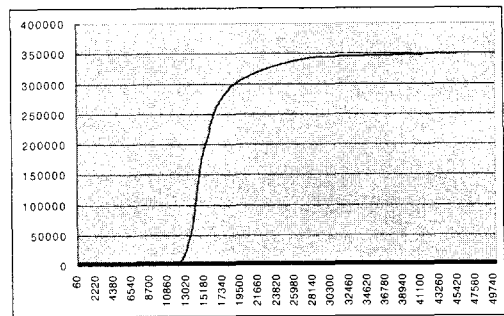
모델링 네트워크의 기본 감염률은 0으로 시작을 하고, 패킷 네트워크에서 웜의 전파가 이루어짐에 따라 웜의 감염률을 계산하여 모델링 네트워크에 전달하는 방식을 사용하였다.

4.3 시뮬레이션 결과

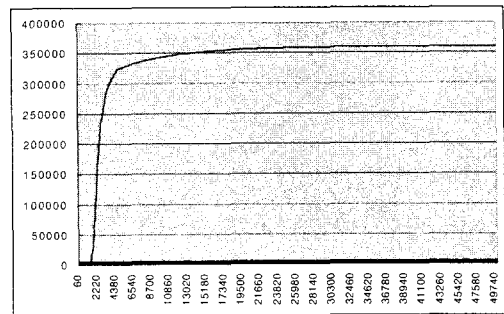
그림 2^[6]와 그림 3은 실제 웜이 전파된 그래프와 그 웜을 모델링 시뮬레이션을 수행하였을 때의 그래프이다. 이 그래프들을 보면 웜의 전파는 그림 2에서는 14시경 급격히 증가하여 24시정도까지 약 10시간 정도동안 전파가 급격히 되는 것을 알 수 있다. 이와 비교하여 그림 3에서는 전파의 시작이 약 20000초에 시작하여 50000초를 조금 지날 때까지 웜이 전파되게 된다. 그림 3의 약 30000초를 시간으로 환산하면 8시간이 좀 넘어가게 되는데 그림 3에서는 50000초일 때도 그래프가 약간 증가하고 있는 상황임을 감안하면 그림 2와 그림 3에



[그림 4] Code-Red worm 형식의 패킷 네트워크



[그림 5] 수정된 패킷 네트워크 I



[그림 6] 수정된 패킷 네트워크 II

서의 감염 그래프는 거의 유사하다고 할 수 있다. 이 두 그래프의 비교를 통하여 이번 실험에서 사용하는 모델링 네트워크의 적합성을 알 수 있게 되었다.

그림 4는 패킷 네트워크를 이용한 네트워크 모델링 시뮬레이션의 결과이다. 패킷 네트워크에서 웜의 전파 방법을 code-red worm과 비슷하게 설정을 하였기 때문에 그 결과 그림 4의 그래프는 그림 3의 그래프와 거의 동일함을 알 수 있다. 그러므로 패킷 네트워크를 정확히 구성한다면 네트워크 모델링 시뮬레이션에 올바른 네트워크 정보가 업데이트 되어 원하는 시뮬레이션을 수행할 수 있다는 것을 보여준다.

그림 5와 그림 6은 패킷 네트워크의 웜 전파 방법을

수정을 하여 시뮬레이션을 수행한 결과이다. 여기서는 같은 모델링 네트워크를 사용한다 하여도 패킷 네트워크의 수정만으로도 다른 결과의 시뮬레이션을 수행할 수 있다는 것을 보여주게 된다.

5. 결론

대규모 네트워크의 시뮬레이션을 수행 하는데 몇 가지 어려움이 따르게 된다. 긴 시뮬레이션 수행 시간, 네트워크 구성의 어려움과 같은 문제점이 존재하게 된다. 또, 모델링 시뮬레이션을 수행하게 되면 그 반대의 문제가 발생하게 된다.

본 논문에서 제안한 방법을 사용하여 시뮬레이션을 수행하게 되면 두 방법의 문제를 패킷 네트워크와 모델링 네트워크가 보완을 하여 효과적인 시뮬레이션을 수행할 수 있도록 해준다.

하지만 이 방법은 시뮬레이션이 패킷 네트워크에 의존을 많이 하기 때문에 패킷 네트워크의 크기 선택 방법과 같이 정확한 패킷 네트워크를 구성하기 위한 방법에 대한 연구를 진행하면 더 정확한 결과의 시뮬레이션을 수행할 수 있을 것으로 생각된다.

6. 참고문헌

[1] David Moore, VernPaxson, Stefan Savage, Colleen Shannon, Stuart Staniford, Nicholas Weaver. "The Spread of the Sapphire/Slammer Worm". CAIDA Technical report, 2003.

[2] 조재익, 임을규, 서정택, 김동수, 박웅기. "Hybrid 모델을 통한 대규모 네트워크 모델링". 한국통신학회 추계종합학술발표회, 2005.

[3] Kalyan S. Perumalla, Srikanth Sundaragopalan. "High-Fidelity Modeling of Computer Network Worms". 20th Annual Computer Security Applications Conference(ACSAC), 2004.

[4] SSFNet Web page. www.ssfnet.org

[5] Michael Liljenstam, David M.Nicol, Vincent H.Berk, Rovert S.Gray. "Simulating Realistic Network Worm Traffic for Worm Warning System Design and testing". WORM, 2003.

[6] David Moore, Colleen Shannon. "The Spread of the Code-Red Worm (CRvw)". CAIDA Analysis page. www.caida.org/analysis/security/code-red/coderedv2_analysis.xml