제28회 한국정보처리학회 추계학술발표대회 논문집 제14권 제2호 (2007. 11)

Bio-IDS 시뮬레이터를 위한 Visualization Tool의 설계 및 구현

문주선, 배장호, 낭종호
서강대학교 컴퓨터공학과
e-mail : {serenity0605, louisv5}@mlneptune.sogang.ac.kr, jhnang@sogang.ac.kr

Design and Implementation of a Visualization Tool for a Simulator of a Bio-Intrusion Detection System

Joo-Sun Moon, Jang-Ho Bae, Jong-Ho Nang
Dept. of Computer Science & Engineering, Sogang University

요 약

본 논문에서는 대규모 네트워크 상에서 발생되는 시뮬레이션 결과를 효과적으로 보여주기 위한 Visualization Tool 을 제안한다. 복잡하고 다양한 시뮬레이션 결과를 얻기 위해, 생태계 모방형 플랫폼을 이용한 Bio-IDS (Intrusion Detection System) 시뮬레이터의 실험 데이터를 이용하였다. 대규모 네트워크를 모두 보이기에는 화면이 너무 작기 때문에, Visualization Tool 은 화면의 확대 및 축소를 위한 Zoom In/Out 기능, 화면의 Panning 을 위한 Scroll Bar 및 현재 영역의 위치를 알려주는 Mini Map 이 필요하였다. 또한, 사용자가 쉽게 시뮬레이션의 속도를 조절할 수 있도록 Simulation Speed Control 기능을 구현하였으며, 각 노드의 효과적인 정상 및 침입 상태 표시를 위한 Icon, 각 노드의 진화 정도와 침입 탐지 정확도를 알려주는 Evolution Number 와 Accuracy Gauge, 해당 시뮬레이션의 결과를 도시하기 위한 Simulation Graph 도 추가하였다. 네트워크 Off-line 환경도 대비하여, DB 로부터의 데이터 입력뿐만 아니라 Log File 을 통한 데이터 입력도 가능하게 하였다. 끝으로, 전체 Node 들의 다양한 상태변화를 확인할 수 있는 Topology Window 와 Simulation Demo Window 간의 Synchronization 을 위한 Socket 통신 등 다양한 기능들이 통합된 Visualization Tool 을 개발함으로써, 대규모 네트워크 시뮬레이션의 효과적인 시뮬레이션이 가능하게 되었다. 이로 인해 대규모 네트워크 상의 복잡한 시뮬레이션 결과도 사용자가 매우 쉽게 파악할 수 있 매우 효과적으로 사용자가 파악할 수 있게 되었다.

1. 서론

생태계 모방 계산모델[1]은 주로 대규모 시스템에서 동작하는 응용/시스템 소프트웨어에 대한 해결책으로 쓰인다. 이러한 응용의 하나로 생태계 모방 플랫폼과 침입탐지 시스템을 결합한 Bio-IDS (Biological Intrusion Detection System)가 있다. 네트워크 상의 패킷을 분석하여 특정 네트워크 패킷이 정상인지 비정상인지에 대한 판단을 내리게 되는 Bio-IDS 는 시뮬레이션 성능과 더불어 효과적인 Visualization 기능 또한 중요하다. 열 번 듣는 것보다 한 번 보는 것이 더 낫기 때문이다. 따라서 Visualization Tool 을 개발하기 위해서는, 대규모 네트워크 상에서의 시뮬레이션 결과를 사용자에게 어떻게 효과적으로 보여줄 수 있을지, 시뮬레이션 성능 분석을 위한 그래프 표현은 어떻게 처리해야 할지 다양한 표현 수단에 대한 이슈들을 고려해야 한다.

여러 가지 표현 수단에 관한 기능들을 검증한 결과, 먼저 대규모 네트워크에서 관심 있는 영역을 표현할 수 있는 Zoom/Scroll 기능이 필요하다. 그리고 Zoom In 상태에서 화면에 보이는 영역이 전체 이미지 중 어느 부분에 속하는지 알려주는 Mini Map 기능 및 시뮬레이션 속도를 빠르게 혹은 느리게 조절할 수 있는 Simulation Speed Control 기능도 필요하다. 다양한 침입 유형과 시스템의 상태 변화를 빨리 파악하기 위해서는 각 Node 들을 Icon 으로 표현하는 것이 효과적이며, 시뮬레이션 결과를 바탕으로 성능상의 변화를 측정하기 위한 Simulation Graph 기능도 생각해야 한다. 마지막으로 네트워크가 Off-line 상태가 될 것을 대비하여, Visualization 을 위한 입력 데이터 처리는 Database 를 통한 접근뿐만 아니라 Log 파일을 통해서도 처리할 수 있어야 하며, 다이내믹한 Visualization Tool 의 효과를 위해 Topology 창과 Simulation Demo 창 간의 Synchronization 이 필요하다.

실험 결과 100,000 개의 네트워크 노드 상에서도 Visualization Tool 이 정상적으로 동작하는 것을 확인하였으며, 사용자의 편의와 이해를 위해 최대한 단순하고 직관적으로 설계하였다.

2. Visualization을 위한 고려사항

네트워크 시뮬레이션은 복잡한 네트워크 구조 상에서의 수 많은 통신과 이벤트들이 각 노드간에 발생된다. 이러한 시뮬레이션 결과를 사용자가 효과적으로

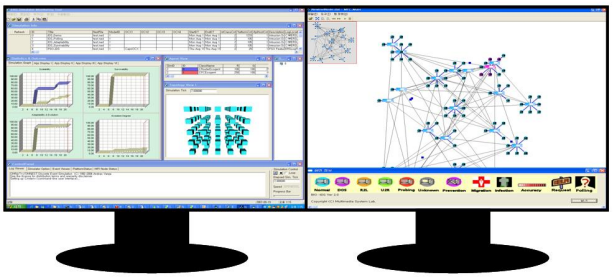
분석하기 위해서는 다음과 같은 3 가지 특징을 고려해야 한다.

· **Scalability** – 복잡한 대규모 그래프 및 네트워크를 모니터 한 화면에 표현할 수는 없다. 수 많은 Node 와 Edge 로 인해 실제 그래프의 구조를 파악하기 어렵기 때문이다. 따라서 스케일에 상관 없이 대규모 이미지의 전체 혹은 일부를 자유롭게 볼 수 있는 기능이 필요하다. 또한 여러 개의 시뮬레이션 결과 창들은 서로 Synch 가 맞아야 한다.

· **Readability** – 수 많은 시뮬레이션 결과를 한 화면에 보여주어야 하기 때문에, 문자나 숫자와 같은 표현 보다는 Symbol 이나 Animation 표현이 필요하다. 또한 색 구분을 통해 다양한 상태 변화를 빠르게 인식할 수 있어야 한다. 또한, 되도록 단순하게 시스템을 설계할수록, Readability 는 높아지게 된다.

· **Survivability** – 시스템의 일부에 오류가 생긴다 해도 전체 시스템의 동작이 멈춰서는 안 된다. 만약 네트워크 연결이 모두 끊겨서 Database 를 사용할 수 없게 되도, Log File 과 같은 대체 수단을 이용해서 Visualization 기능을 수행할 수 있어야 한다.

3. Bio-IDS Visualization Tool 을 위한 기능 설계 및 구현

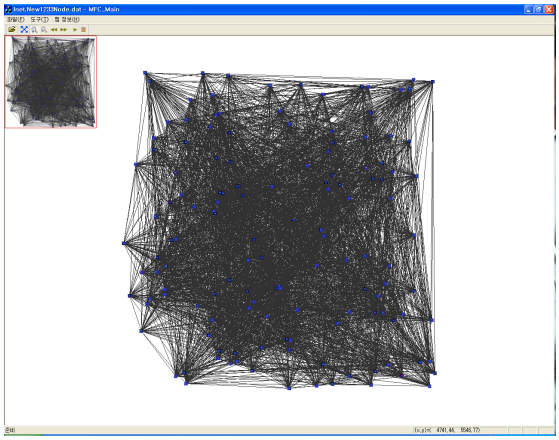


(그림 1) Dual Monitor 상에 나타난 Bio-IDS Visualization Tool 의 전체 GUI

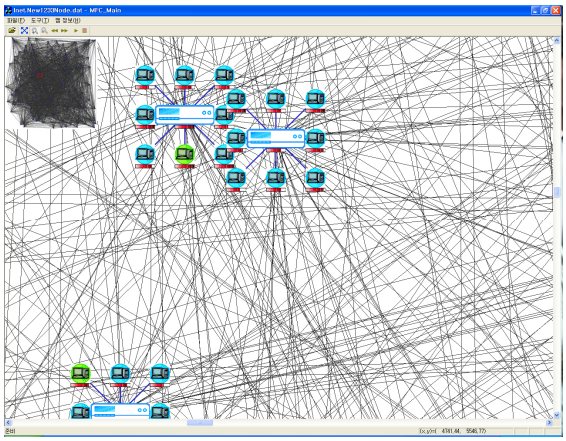
(그림 2) Bio-IDS Visualization Tool 의 GUI 설명

Bio-IDS 에서는 네트워크의 Router 들과 각 Router 에 연결된 Terminal Node 들을 표현한다. 이를 실제 연결 상태와 가깝게 표현하기 위해서는 화면 상에 수많은 Node 들이 나타나야 한다. 또한 시뮬레이션 결과에 따른 생태계 모방형 시스템의 확장성, 생존성, 적응성 및 진화성을 표현할 수 있는 결과 화면이 필요하다. 앞에서 언급한 Visualization Tool 의 세가지 고려사항, Scalability, Readability, and Survivability 기능들을 효과적으로 표현하도록 구현한 전체 Bio-IDS Visualization Tool 의 모습은 (그림 1)과 (그림 2)에서 볼 수 있다. 다양한 정보를 한 화면에 표현하기 위해, Dual Monitor 를 사용하였으며, (그림 2)는 각 화면의 작은 창들에 대한 설명이다.

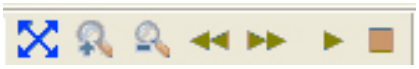
3.1. Zoom & Scroll Bar



(그림 3) 1000 개의 노드에 대한 시뮬레이션 데모 창



(그림 4) Zoom In 된 시뮬레이션 데모 창



(그림 5) 도구 모음 창

실제 네트워크의 Node 들은 Router 와 Terminal 을 합쳐 그 수가 매우 크기 때문에, 화면에 표시할 경우 Packet 의 이동이나 상태 변화가 너무 작아서 눈으로 확인하기가 쉽지 않고, 그래프의 Edge 들간의 간격이 너무 조밀해서 가독성이 떨어지는 단점이 있다. 이러한 문제를 해결하기 위해, (그림 5)의 Zoom 버튼과 (그림 4)의 Scroll Bar 기능을 추가하였다.

3.2. Mini Map

Zoom 버튼을 통해 전체 네트워크 그래프를 확대하였을 때, 화면에 보이는 영역이 전체 그래프의 어느 부분인지 표현하기 위하여, (그림 4)의 좌측 상단에서 보여지는 것처럼 Mini Map 을 통해 확인할 수 있도록 구현하였다. Mini Map 은 전체 네트워크 그래프를 축소한 이미지 위에, 빨간색의 네모 칸을 표시하여 현

재 시뮬레이션 대모 창에 보이는 영역이 전체 영역 중 어느 부분에 속하는지 알 수 있도록 표시하였다.

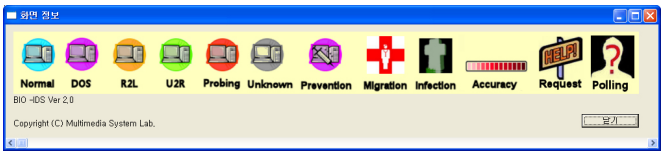
3.3. Simulation Speed Control

(그림 5)의 오른쪽 부분에서 볼 수 있듯이, 사용자가 자신이 원하는 속도로 시뮬레이션 결과를 확인할 수 있도록 Speed Control 버튼을 구현하였다. 시간 간격은 1 배속, 2 배속, 4 배속, 8 배속 및 최대 16 배속까지 속도를 조절할 수 있다. 만약 매 1 초마다 각각의 frame 을 보여줘야 하는데, 중간에 몇 frame 을 skip 하거나 건너 뛴다면, 전혀 엉뚱한 결과를 보여줄 수 있다. 어떤 터미널이 Node 가 외부로부터 침입을 받는 장면이 나오지도 않았는데, 시스템에 공격 당해서 갑자기 고장 나는 시나리오가 나올 수 있기 때문이다. 따라서, Sleep 함수의 시간 파라미터를 조절해서, 모든 상황 정보를 화면에 보여주되 그 변화만 빠르게 구현하는 방식이 사용자에게 정확한 시뮬레이션 결과를 보여주는데 효율적이다.

3.4. Icon and Help Window

<표 1> 침입 유형에 따른 아이콘(Icon) 및 상태 정의

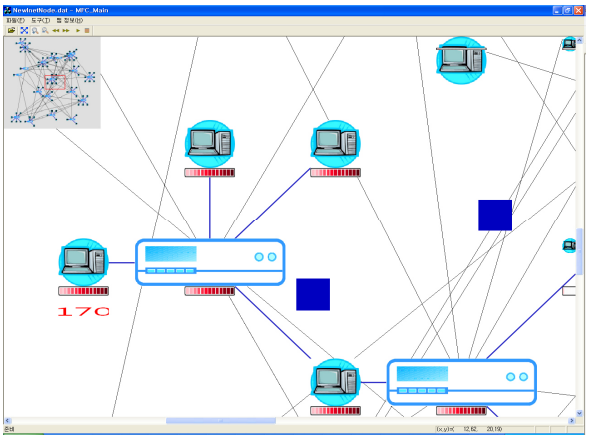
Icon	Color	Status	Definition
	Cyan	Normal Connection	정상 패킷
	Pink	DoS Intrusion	서비스 거부
	Orange	R2L Intrusion	외부로부터의 비인가 접근
	Green	U2R Intrusion	Root 권한에 대한 비인가 접근
	Red	Probing Intrusion	감시 및 Probing
	Gray	Unknown	미확인 패킷



(그림 6) 도움말 창

<표 1>에서 보이는 바와 같이, Node 의 상태는 Normal Connection, DoS, R2L, U2R, Probing, Unknown 과 같은 6 가지의 상태를 가진다. 4 개의 침투 유형은 1999 년 Lincoln Laboratory DARPA Intrusion Detection System 에서 정의한 Evaluation Data Set[2,3]을 따랐다. 여기에 정상인지 비정상인지 판단할 수 없는 Unknown Status 와 정상 상태인 Normal Connection 아이콘을 추가하였다. 각 Node 의 상태는 화면에서의 Node 크기가 작아지더라도 단번에 각 상태에 대한 정보를 파악할 수 있도록, 서로 다른 6 가지의 색으로 구분하였다. 이외에도 (그림 6)에서 볼 수 있듯이, Bio-IDS 시뮬레이션을 위한 다양한 아이콘들이 있다. 시뮬레이션 데모 창에 불필요한 창들이 많이 보이면, 실제 시뮬레이션 결과를 확인하는데 어려움이 많으므로, 도움말 창은 언제든지 필요할 때 불렀다가 다시 지울 수 있도록 Pop-up 형식으로 구현하였다.

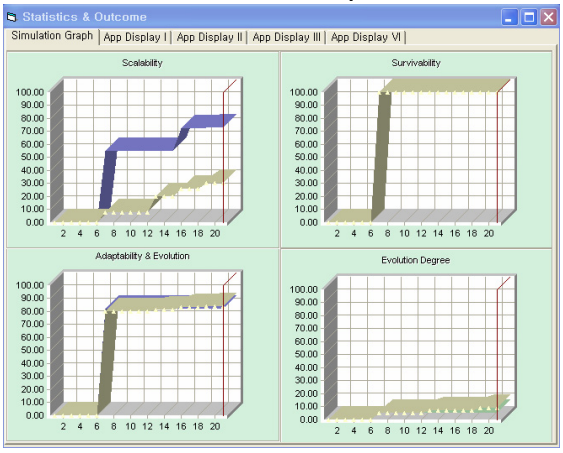
3.5. Evolution Number and Accuracy Gauge



(그림 7) 진화 정도와 IDS 정확도의 표현

생태계 모방형 시스템의 대표적인 특징은 시스템이 스스로 진화할 수 있다는 것이다. 이러한 진화성은, 계속해서 무한한 진화 과정을 거치면서 새로운 Rule 을 만들어내어 알려지지 않은 새로운 유형의 침입을 탐지하거나, 시스템의 탐지 정확도를 향상시킬 수 있다. (그림 7)에서 볼 수 있듯이, 각 플랫폼의 진화 정도는 숫자로, 탐지 정확도는 Accuracy Gauge 로 표현하였다. 진화라는 개념은 끝이 없기 때문에, 일정한 한계 값이 없고 무한히 반복적으로 Evolving 회수만 증가하게 된다. 그러므로 각 플랫폼의 Evolving 정도를 표현하기 위하여 그림에서 볼 수 있듯이 그림 아래에 숫자를 표현하였다.

3.6. Simulation Performance Graph



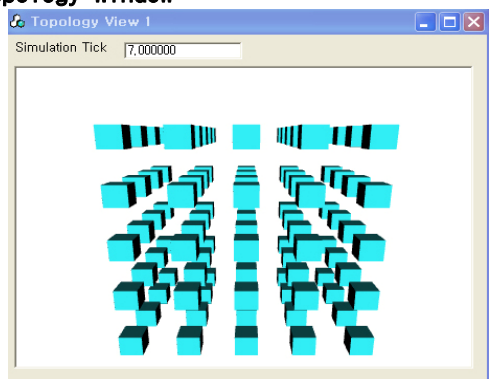
(그림 8) 시뮬레이션 성능 그래프

시뮬레이션 결과값들을 일렬로 나열한다면, 그 결과가 어떤 성능을 보이는지 쉽게 알 수 없다. 따라서 이러한 시스템 성능의 가독성을 높이기 위해서는 (그림 8)과 같은 그래프 형태로 바꾸는 것이 효과적이다. 생태계 모방형 시스템의 특징은 확장성과 적응성, 생존성 및 진화성인데, 일반적인 IDS 와 생태계 모방 플랫폼을 접목한 Bio-IDS 와의 성능 차이를 나타내었다.

3.7. Input Data Processing for On/Off-line

Visualization Tool 은 일부 시스템의 제약이 따르더라도 전체 기능에 문제가 없는 Survivability 기능이 필요하다. 때문에 기본 방식은 On-line 환경에서 Database 로부터 Simulation 결과값을 불러오는 것이지만, 네트워크 환경이 끊기거나 불안정 할 경우 Off-line 환경에서 Log file 을 읽어 Visualization Tool 이 동작할 수 있도록 설계하였다.

3.8. Topology Window



(그림 9) 토폴로지 창

(그림 9)에서 볼 수 있듯이, 시뮬레이터의 각 Node 들을 하나의 Grid Topology 로 표현하였다. 이렇게 표현하였을 경우, 각 Node 들의 상태 변화를 한눈에 관찰할 수 있기 때문이다. 이 토폴로지 창은 Zoom, Pan, Roll, Rotation 이 가능하여 사용자에게 Dynamic 한 Visualization 을 제공한다.

3.9. Synchronization

Visualization Tool 은 (그림 1)에서 볼 수 있듯이 크게 좌측의 전체 Simulation 을 관리하는 창과 우측의 Simulation Demo 창으로 나뉘어진다. 좌측 창의 경우 4 가지 속성의 Simulation Graph 및 다양한 시뮬레이션 진행 상황을 알려주는 등, Window 가 너무 많아 가독성이 떨어진다. 따라서, 시뮬레이션의 효과적인 Visualization 을 위해, Simulation Demo 를 위한 새로운 응용창을 우측 화면에 만들었다. 이러한 여러 개의 시뮬레이션 결과 창들간의 Synch 를 맞추기 위해서, Winsock 을 이용한 Client-Sever 의 socket 통신을 이용하였다. 이를 채택한 이유는 각 창들간의 Synch 가 하나의 PC 에서 이루어지므로, 내부적인 Socket 통신에 따른 jitter 를 무시 할 수 있고, 비교적 간단하게 구현이 가능하기 때문이다. 처음 Tool 을 초기화하면, 좌측의 창과 시뮬레이션 데모 창과의 상호 통신을 위한 Socket 을 서로 열게 된다. 이후, 좌측의 시뮬레이션 정보 창에서 응용 하나가 선택되면, 두 창간의 네트워크가 실제로 연결된다. 우측 창의 Socket 은, Asynchronous Socket Class 를 이용하였다. 이를 채택한 이유는, 하나의 PC 상에서 시간간격이 일정한 내부적인 Socket 통신을 하기 까닭에, 전체 Message 가 오류없이 온전히 전달될 수 있기 때문이다. 데모를 실행하게 되면 좌측 창에서 현재 일어나고 있는 Simulation 에 대한 정보를 Simulation 의 1 step 마다 우측 창으로 보낸다. 우측 창에서는 수신한 정보에 따라서 그에 맞는 Simulation Demo 를 1 step 단위로 수행한다.

4. 결론

그림 한 장은 수 많은 글보다 단시간 내에 더 많은 정보를 사용자에게 효과적으로 알려준다. 때문에 사용자의 편의성과 직관성을 고려한 Visualization Tool 의 설계는 실제 Simulator 의 설계와 성능만큼이나 중요한 작업이다. 대규모 네트워크 상에서 발생되는 시뮬레이션 결과를 효과적으로 보여주기 위해, 생태계 모방형 플랫폼을 이용한 Bio-IDS 시뮬레이터의 시뮬레이션 결과를 분석할 수 있는 Visualization Tool 을 개발하였다. 대규모 네트워크를 모두 보이기에는 화면이 너무 작기 때문에, Visualization Tool 은 화면의 확대 및 축소를 위한 Zoom In/Out 기능, 화면의 Panning 을 위한 Scroll Bar 및 현재 영역의 위치를 알려주는 Mini Map 이 필요하였다. 또한, 사용자가 쉽게 시뮬레이션의 속도를 조절할 수 있도록 Simulation Speed Control 기능을 구현하였으며, 각 노드의 효과적인 정상 및 침입 상태 표시를 위한 Icon, 각 노드의 진화 정도와 침입 탐지 정확도를 알려주는 Evolution Number 와 Accuracy Gauge, 해당 시뮬레이션의 결과를 도시하기 위한 Simulation Graph 도 추가하였다. 네트워크 Off-line 환경도 대비하여, DB 로부터의 데이터 입력뿐만 아니라 Log File 을 통한 데이터 입력도 가능하게 하였다. 끝으로, 전체 Node 들의 다양한 상태변화를 확인할 수 있는 Topology Window 와 Simulation Demo Window 간의 Synchronization 을 위한 Socket 통신 등 다양한 기능들이 통합된 Visualization Tool 을 개발함으로써, 대규모 네트워크 시뮬레이션의 효과적인 시뮬레이션이 가능하게 되었다. 이 Tool 을 이용하여 복잡한 시뮬레이션 결과를 쉽고 빠르게 사용자에게 전달할 수 있었다.

참고문헌

[1] M. Wang and T. Suda, “The Bio-Networking Architecture: A Biologically Inspired Approach to the Design of Scalable, Adaptive, and Survivable/Available network Application,” *Proc. of the IEEE Symposium on Application and the Internet*, 2001.

[2] Richard Lippmann, Joshua W. Haines, David J. Fried, Jonathan Korba, Kumar Das "The 1999 DARPA Off-Line Intrusion Detection Evaluation", *Draft of paper submitted to Computer Networks*, In Press, 2000.

[3] Lincoln Laboratory, http://www.ll.mit.edu/IST/ideval/