論文
5-2-6

다양한 연동 구조를 통한 보안 시스템의 성능 비교 (Performance Comparison of Security System with Various Collaboration Architecture)

김 희 완(Hee-Wan Kim[1]), 서 희 석(Hee-Suk Seo)[2]

요 약

e-비즈니스의 급격한 발전으로 인하여 네트워크 상의 보안이 중요한 이슈로 부각되고 있다. 대표적인 보안 시스템인 침입 탐지 시스템(IDS)은 네트워크 상의 침입 시도를 탐지하는 역할을 수행한다. 현재의 침입은 광범위해지고, 복잡하게 되어 한 침입 탐지 시스템이 독립적으로 네트워크의 침입을 판단하기 어렵게 되었다. 그래서 본 논문에서는 여러 침입 탐지 시스템을 네트워크 상에 배치하였고, 이들이 서로 정보를 공유하면서 공격자에 효과적으로 대처하며 침입을 탐지하도록 하였다. 각 에이전트들이 침입을 탐지하기 위한 연동 방법은 블랙 보드 구조(Blackboard Architecture)와 계약망 프로토콜(Contract Net Protocol)을 사용하였다. 본 논문에서는 보안 에이전트들이 블랙 보드 구조를 사용한 경우와 계약망 프로토콜을 사용한 경우의 성능을 비교해 효과적인 방법을 제안할 것이다.

ABSTRACT

As e-business being rapidly developed the importance of security is on the rise in network. Intrusion detection systems which are a core security system detect the network intrusion trial. As intrusions become more sophisticated, it is beyond the scope of any one IDS to deal with them. Thus we placed multiple IDS agents in the network and the information helpful for detecting the intrusions is shared among these agents to cope effectively with attackers. Each agent cooperates through the BBA (Black Board Architecture) and CNP (Contract Net Protocol) for detecting intrusions. In this paper, we propose the effective method comparing the blackboard architecture to contract net protocol.

keywords : collaboration, blackboard architecture, contract net protocol, intrusion detection system, modeling.

1) 정회원 : 삼육대학교 컴퓨터과학과 조교수
2) 정회원 : 성균관대학교 정보통신공학부 박사 과정

논문접수 : 2004. 2. 9.
심사완료 : 2004. 2. 19.

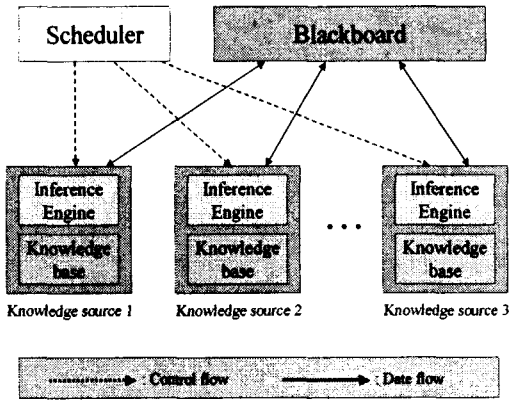
1. 서 론

네트워크 보안 규모가 급속히 확대되고 있다. 대표적인 보안 시스템인 방화벽은 외부 침입을 차단하기 위해 기업 내 네트워크 망과 인터넷이라는 외부 공개망의 접점에 위치한 기업 보안의 일차 저지선이다 [1-3]. 그러나 인터넷 발전과 급속하게 발전하고 있는 해킹 기술의 발전에 따라 방화벽만으로는 다양한 기술과 방법론으로 무장한 해커의 침입을 차단하는데 한계가 있다. 또한 해킹이 외부 사용자뿐만 아닌 내부 사용자에 의한 경우가 많아 방화벽만으로는 내부 사용자의 해킹 행위에 100퍼센트 무방비 상태로 당할 수 밖에 없다. 침입 탐지 시스템은 침입 차단 시스템이 효과적인 차단에 실패하였을 경우 이에 따른 피해를 최소화하고 네트워크 관리자 부재 시에도 해킹에 적절히 대응할 수 있는 보안 솔루션에 대한 요구가 증가하고 있기 때문이다. 침입 탐지 시스템은 침입 차단 시스템이 단순한 룰에 따라 불법 침입을 차단하는데 따른 보안상의 한계점을 보완한다 [4-6].

다중 에이전트의 연구에서 분산 인공지능(Distributed Artificial Intelligence)의 새로운 기술에 대한 연구가 인공지능의 연구에서 중요한 분야가 되고 있으며 본 논문에서는 보안 시스템의 연동을 위해 블랙보드 구조와 계약망 프로토콜을 적용할 것이다 [7,8]. 블랙보드 구조는 네트워크 상의 공유메모리인 블랙보드를 활용하여 각 에이전트들이 서로 정보를 공유할 수 있도록 구성한 연동 구조이다. 계약망 프로토콜은 분산된 에이전트들 중에서 bidding의 과정을 통해서 최상의 에이전트를 선택하고 선택된 에이전트는 서비스를 제공하게 된다 [9-11].

2. 관련 연구

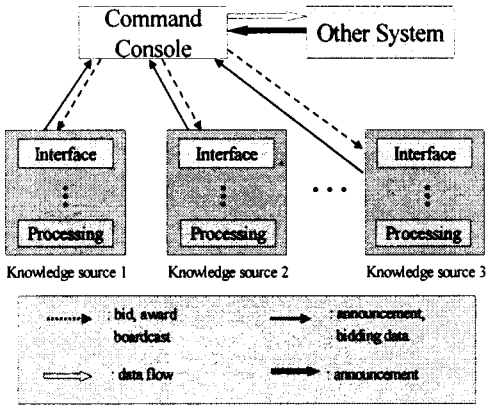
2.1 블랙 보드 구조



[그림1] 블랙보드 구조의 구성

분산 인공 지능의 한 영역인 블랙보드구조는 분산된 에이전트들이 공동 작업을 통하여 문제를 해결하기 위한 방법을 제공한다. 블랙보드구조의 한 요소인 블랙보드는 문제에 적합한 추상화된 몇 개의 레벨로 분할되어 있다. 특정한 레벨을 통해 통신을 수행하던 에이전트들은 상호작용을 통하여 인접한 레벨로 전이할 수 있다. 이러한 방법을 통해 에이전트들이 수집한 데이터는 한 레벨을 통해 공유되고, 이렇게 공유된 데이터들을 활용하여 목표로 하는 단계로의 전이를 할 수 있다. 일반적으로 목표 레벨은 바로 찾아가기 어려운 작업으로 여러 에이전트들이 서로 조금씩 일을 분담하여 처리하여 그 결과를 블랙보드를 통해 공유하여 최종적으로 목표에 이르고자하는 방법이다. 블랙보드구조의 단순성으로 인해 분산 인공 지능 분야에서 많이 사용되는 개념이다.

2.2 계약망 프로토콜(Contract Net Protocol)



[그림 2] 계약망 프로토콜의 구성

계약망 프로토콜은 분산된 문제(distributed problem)를 해결하는데 있어 에이전트들 사이의 통신을 하기 위한 도구로서 제안되었다. 작업의 분산을 통해 각 에이전트들은 효과적으로 주어진 작업을 처리한다. 또한 자신이 처리하지 못하는 작업의 경우는 다른 에이전트에게 의뢰하여 처리하므로 자신이 처리할 수 없는 작업의 처리도 가능하다. 이와 같은 특성을 침입 탐지에 적용하게 되면 신속하고 정확한 탐지가 가능하며 무엇보다도 새로운 침입을 탐지하는 능력을 향상시킬 수 있다. 계약망 프로토콜의 사용은 분산 감지 시스템과 분산 전달 시스템을 위해서 시도 되었다. 계약망 프로토콜은 에이전트들이 계약(contract)에 의하여 분산된 문제를 해결하기 위하여 협상하고 통신하는 메커니즘을 제공한다. 에이전트들은 수행될 필요가 있는 작업을 알리고 다른 에이전트들에게 공지된 작업들을 수행하기 위해 bid를 만들어서 보내면 커맨드 콘솔(Command Console)은 각 에이전트들이 제출한 bid를 평가하여 최상의 에이전트를 선택하여 계약을 체결하게 된다. 계약망 프로토콜의 적용은 다중 침입 탐지 시스템에 있어서 서로 보완하고 협력하여 탐지의 성능을 향상시키고 정확도를 높일 수 있다.

2.3 침입 탐지 시스템

침입 탐지 시스템은 단순한 접근 제어 기능을 넘어서 침입의 패턴 데이터베이스와 전문가 시스템을 사용해 네트워크나 시스템의 사용을 실시간 모니터링하고 침입을 탐지하는 보안 시스템이다. 침입 탐지 시스템은 허가되지 않은 사용자로부터 접속, 정보의 조작, 오용, 남용 등 컴퓨터 시스템 또는 네트워크 상에서 시도됐거나 진행 중인 불법적인 예방에 실패한 경우 취할 수 있는 방법으로 의심스러운 행위를 감시하여 가능한 침입자를 조기에 발견하고 실시간 처리를 목적으로 하는 시스템이다.

침입이란 시스템에 대한 고의적 불법적인 행위를 말하며 시스템의 불법 침입, 중요 정보의 유출 및 변경, 훼손, 불법적인 사용, 그리고 컴퓨터 바이러스 및 서비스거부 등과 같은 구체적인 형태로 나타난다. 침입 탐지 시스템은 이러한 불법적인 침입행위를 신속하게 감지하고 대응하는 소프트웨어를 말하며 간단하게는 로그 파일 분석에서부터 복잡한 실시간 침입 탐지 시스템까지 다양한 소프트웨어가 존재한다. 침입 탐지 기법은 크게 비정상적인 침입 탐지 기법과 오용 침입 탐지 기법으로 나눌 수 있다.

침입 탐지 시스템은 모니터링의 대상에 따라 <표 1>과 같이 네트워크 기반 침입 탐지 시스템과 호스트 기반 침입 탐지 시스템으로 나눌 수 있다.

1. 호스트 기반 IDS (H-IDS) : 시스템 내부에 설치되어 하나의 시스템 내부 사용자들의 활동을 감시하고 해킹 시도를 탐지해내는 시스템이다. 각종 로그 파일 시스템 콜 등을 감시한다.
2. 네트워크 기반 IDS (N-IDS) : 네트워크의 패킷 캡처링에 기반하여 네트워크를 지나다니는 패킷을 분석해서 침입을 탐지해낸다.

항목	N - IDS	H - IDS
탐지 대상	네트워크를 통과하는 패킷	시스템 내부 사용자들의 활동
설치 단위	네트워크	세스먼트 호스트
기반 기술	패킷 캡처링	프로세스 모니터링
	프로토콜별 패킷 분석	실시간 로그분석
	패킷 조각 모음	TTY모니터링

[표 1] IDS의 분류

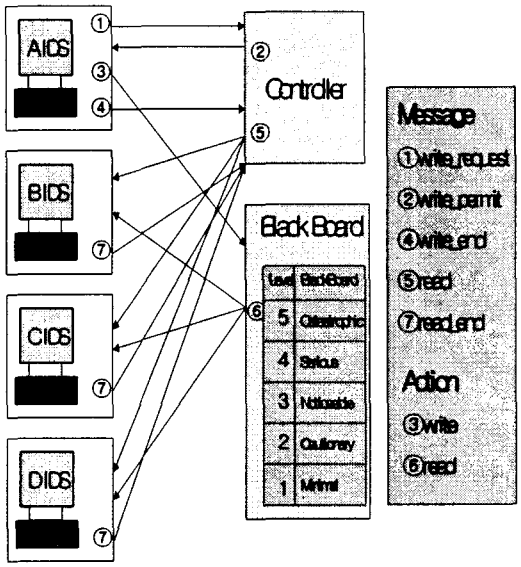
호스트 기반의 침입 탐지 시스템은 시스템 감사를 위해서는 기술적인 어려움이 크고, 비용이 비싸다. 그리고 로그 분석 수준을 넘어 시스템 콜 레벨 감사까지 지원해야 하기 때문에 여러 벤더의 운영 체제를 위한 제품을 개발하는 것 또한 시간적, 기술적으로 어렵다는 단점이 존재한다. 이에 비해 네트워크 기반의 침입 탐지 시스템은 운영 체제의 제약이 없고 네트워크 단에서 독립적인 작동을 하기 때문에 구현과 구축비용이 저렴하다

3. 연동 구조 내의 보안 시스템

3.1 블랙보드 구조를 활용한 보안 시스템 연동

블랙보드 구조는 공유된 지식 구조인 블랙보드를 사용하여 통신이 이루어지므로, 각 에이전트가 블랙보드에 쉽게 내용을 게재하고, 다른 에이전트에 의해 게재된 내용을 쉽게 열람할 수 있다. 블랙보드의 단계(level)는 Joseph Barrus & Neil C. Rowe가 제안한 Danger values에 의해 5가지 단계로 정의하였다.

Danger values are:
- Minimal
- Cautionary
- Noticeable
- Serious
- Catastrophic



[그림 3] IDS와 BBA 간의 메시지 교환

Minimal 단계는 확실하게 알려진 공격인지를 확인할 수 없는 단계이고, Cautionary는 Minimal 단계가 계속되는 단계이다. Noticeable 단계는 알려진 공격인지를 확실하게 알 수 있고 잠정적으로 피해를 줄 수 있는 단계이다. Serious 단계는 네트워크에 큰 피해를 줄 수 있는 단계이고, Catastrophic 단계는 네트워크에 참혹한 피해(catastrophic losses)를 줄 수 있는 단계이다. 본 논문에서는 이런 단계를 임계값을 통해 구분하였다.

각 침입 탐지 에이전트와 블랙보드의 통신에 사용되는 메시지는 제어 메시지와 데이터 메시지가 있다. 하나의 침입 탐지 에이전트가 블랙보드에 메시지를 게재하기 위해서는 제어기(Controller)에게 쓰기(write)를 요청해 승인을 받은 후 블랙보드에 쓰기를 하게 된다. 쓰기가 끝나면 write_end 메시지를 제어기에게 보내고

제어기는 다른 침입 탐지 에이전트에게 읽기(read)를 통보한다. 읽기가 끝난 침입 탐지 시스템은 read_end 메시지를 제어기에게 보낸다. [그림 3]은 이러한 트랜잭션을 보여준다.

```
IDAMailBomb::IDAMailBomb():
IDATwo()
{
m_PSR = new MailBombRule;//rule을 생
성
}

IDAMailBomb::~IDAMailBomb()
{
delete m_PSR;//rule 파괴
}

void IDAMailBomb::SetView(CView* v)
{
m_View = (CEditView *)v;
  //view에 대한 포인터를 얻어 옴.
m_PSR->SetView(v);
  //rule에서도 view를 접근하도록 view
포인터를 넘겨 줌.
}

void  IDAMailBomb::InferStart(DataList*
imsy)
{
...

DataList *print = imsy;
if(print==NULL||print->IsEmpty())
 ... //null 이라는 메시지 출력
else{
  while( !(print->IsEmpty()) ){
    Slot_List fact;
    MakeFact(print,fact);
      //전문가시스템의 사실 생성
...
   if( m_PSR->Inference(fact) ){
     if(alarm==0) //침입 탐지를 알림.
    }
    print = print->GetNext();
  }//출력하기 위한 while의 끝부분.
 }//end else

...
```

3.2 계약망 프로토콜을 활용한 보안 시스템 연동

내부 네트워크로 패킷이 유입되면 Command Console은 모든 침입 탐지 Agent에게 bid 메시지를 보내고 이 메시지를 받은 Agent들은 bid_data 메시지를 보낸다. Command Console은 bid_data를 가지고 선택 알고리즘에 의해 침입을 탐지할 Agent를 선택하게 되고 선택된 Agent에게 award 메시지를 보낸다. award 메시지를 받은 Agent는 packet_data를 기다리고 Command Console은 패킷 정보를 packet_data에 복사하여 선택된 Agent에게 보낸다. 선택된 Agent는 이 데이터를 가지고 침입을 탐지하게 된다.

침입 탐지 과정 중 Detector 모델에서 상태전이가 발생하여 failed 상태가 되면 Agent는 Command Console에 announcement 메시지를 보내고 이 메시지를 받은 Command Console은 위의 과정과 마찬가지로 다른 모든 Agent에게 bid 메시지를 보내고 Agent 선택과정을 반복하게 된다.

침입을 탐지한 경우에는 선택된 Agent가 intrusion 메시지를 Command Console에 보내고 intrusion_data 메시지를 보낸다. 이 메시지를 받은 Command Console은 Firewall에게 intrusion과 intrusion_data 메시지를 차례로 보내고 모든 침입 탐지 Agent에게 broadcast 메시지와 침입에 대한 정보를 broadcast_data 메시지로 보낸다. 그런 다음 다시 bid 메시지를 보내고 위의 Agent 선택과정을 반복한다.

침입을 탐지하는 전문가 시스템은 규칙의 집

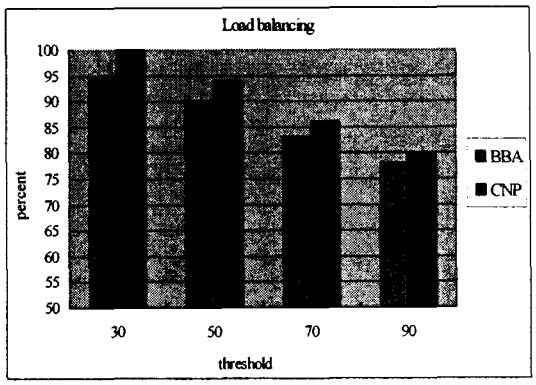
합인 지식 베이스, 추론을 수행하는 추론 엔진 그리고 사실을 저장하는 working memory (WM)로 구성된다. 추론 방식은 전향 추론 방식 (forward chaining inferencing)을 적용하는데 추론과정은 패턴 매칭 (pattern matching), 충돌 해결 (conflict resolution) 그리고 실행 (act)의 순서로 이루어진다. 각 규칙의 left-hand side (LHS)는 규칙에서 if 부분과 일치하는 조건의 결합으로 구성되고 right -hand side (RHS)는 규칙에서 then 부분과 일치하는 일련의 행동들로 구성된다. 패턴 매칭은 규칙에서 LHS와 WM에 있는 사실들을 비교한다. 이 과정의 결과 만족된 규칙이 2개 이상인 경우는 충돌 셋 (conflict set)이 구성된다. 다음에는 미리 정의된 충돌 해결 전략 (conflict resolution policy)에 따라 충돌 셋에서 하나의 규칙을 선택하고 마지막으로 그 규칙의 일련의 행동들를 실행하여 WM에 있는 내용을 변화시킨다. WM는 초기상태에서 추론과정을 통해 규칙을 선택하고 최종적으로 침입을 탐지하게 된다.

4. 시뮬레이션

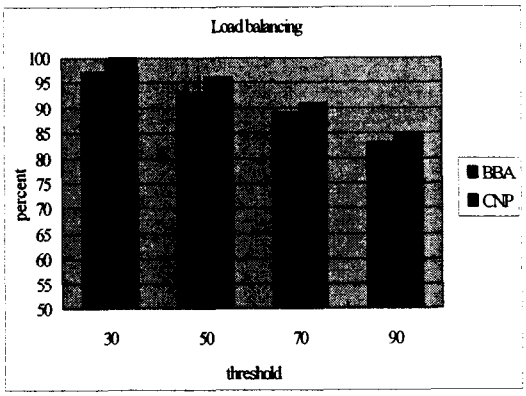
본 연구의 시뮬레이션 수행을 위한 모델은 DEVS (Discrete EVent system Specification) 모델을 사용하여 모델링을 수행하였다. 시뮬레이션을 위해서 침입 탐지 시스템의 모델을 구성하였으며 블랙 보드 구조를 활용하기 위한 블랙 보드 구조 모델과 계약망 프로토콜을 사용하기 위한 모델을 구성하였다. 각 시뮬레이션은 임계값 30, 50, 70, 90으로 구성하였다. 시뮬레이션 수행을 통한 성능 평가 지표로는 로드 밸런스와 침입 탐지율을 선정하였으며, 각 성능 지표에 대해서 연동 구조의 에이전트가 3개인 경우, 4개인 경우에 대해서 시뮬레이션을 수행하였다.

4.1 로드 밸런싱

블랙 보드 구조와 계약망 프로토콜을 사용한 침입 탐지 시스템의 연동 시 두 구조를 사용할 때의 성능 측정을 위하여 각 에이전트에 부과되는 로드(load) 밸런스를 측정하였다. 아래의 각 시뮬레이션 결과에서 로드 밸런스를 비교하기 위하여 임계값 30의 CNP의 로드 밸런스를 기준으로 계산하여 나머지 값들을 계산하였다.



[그림 4] 에이전트가 3개인 경우의 로드 밸런스



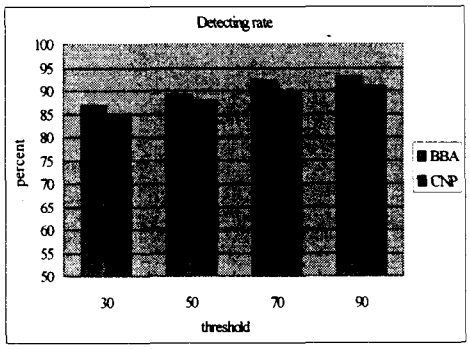
[그림 5] 에이전트가 4개인 경우의 로드 밸런스

블랙 보드 구조와 계약망 프로토콜을 사용한 경우의 로드 밸런스는 계약망 프로토콜을 사용한 경우가 약간 높게 노드 밸런스가 이루어진 것을 볼 수 있다. 이와 같은 결과는 계약망 프로토콜이 전문성을 평가하여 에이전트를 선택하

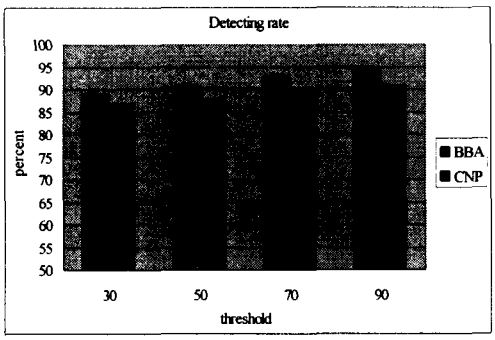
게 되므로 이러한 이점을 통해서 얻어진 결과라고 생각할 수 있다. 또한 에이전트가 3개인 경우보다 4개인 경우의 로드 밸런스가 조금 더 좋은 것을 알 수 있다.

4.2 침입 탐지율

<그림 6,7>에서와 같이 침입 탐지율은 블랙 보드 구조를 사용한 경우의 효율이 조금 더 높음을 알 수 있다. 블랙 보드의 모든 에이전트가 전문성을 고려하지는 않았지만, 대신 모두 침입 탐지에 참여하여 작업을 수행하여 얻어진 결과라고 할 수 있다. 또한 그림에서와 같이 보안 강도를 높일수록 탐지율이 높아짐을 알 수 있다.



[그림 6] 에이전트가 3개인 경우의 침입 탐지율



[그림 7] 에이전트가 4개인 경우의 침입 탐지율

5. 결 론

본 논문에서는 보안 시스템에서 많이 사용되는 분산 침입 탐지 시스템의 성능을 측정하였다. 네트워크의 발전으로 인해서 다수의 분산 침입 탐지 시스템을 통해서 침입을 탐지하게 되면 그 성능을 높일 수 있는 장점이 존재하는데, 이러한 분산 시스템의 연동은 블랙 보드 구조와 계약망 프로토콜을 사용하였다. 블랙 보드 시스템 및 계약망 프로토콜 모두 장점이 존재하게 된다. 블랙 보드 시스템을 사용한 경우는 침입 탐지의 성능이 조금 좋은 것을 알 수 있었다. 또한 블랙 보드는 구조상 블랙 보드의 레벨을 갖을 수 있으므로 레벨에 맞는 정책 적용을 용이하게 수행할 수 있으며, 침입 탐지 시 정책의 적용이 용이하다. 계약망 프로토콜은 각 에이전트에 전문성을 부여하여 우선 전문성을 고려한 탐지를 하게 되므로 로드 밸런스에 유리하다는 측면을 갖는다. 하지만 블랙보드에 많은 트랜잭션을 요구한다는 단점도 존재한다.

참 고 문 헌

[1] 한국정보학회, "차세대 네트워크 보안 기술" 한국정보보호진흥원, 2002.

[2] R. Base. "Intrusion Detection", Macmillan Technical Publishing, 2000.

[3] E. Amoroso, "Intrusion Detection - An Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response", Intrusion.Net Books, 1999.

[4] K. M. Sim, S. K. Shiu, and B. L. Martin, "Simulation of a Multi-agent Protocol for Task Allocation in Cooperative Design," IEEE SMC '99 Conference Proceedings. International Conference on, vol.3, pp. 95-100, 1999.

[5] Jihoon Yang, Raghu Havaldar, Vasant

Honavar, Les Miller and Johny Wong, "Coordination of Distrbuted Knowledge Networks Using Contract Net Protocol," Information Technology Conference, IEEE, pp. 71-74, 1998.

[6] R. Smith, "The Contract Net Protocol: High-level Communication and Control in a distributed problem solver," IEEE Transactions on Computers, vol. C-29, no. 12, pp. 1104-1113, December. 1980.

[7] H. van Dyke Parunak. Manufacturing Experince with the Contract Net. In Research Notes in Artificial Intelligence: Distributed Artificial Intelligence, Vol. 1, pp. 285 - 310, Morgan Kaufmann Publishers, 1987.

[8] S. Northcutt, "Network Intrusion Detection : An Analysts Handbook", New Riders Publishing, 1999.

[9] H.S. Seo and T.H. Cho, "An application of blackboard architecture for the coordination among the security systems", Simulation Modelling Practice and Theory, Elsevier Science B.V., vol. 11, issues 3-4, pp. 269-284, Jul. 2003.

[10] B. P. Zeigler, H. Praehofer, T. G. Kim, Theory of Modeling and Simulation, 2nd Ed., Academic Press, 2000.

[11] T.H. Cho and Bernard P. Zeigler, "Simulation of Intelligent Hierarchical Flexible Manufacturing: Batch Job Routing in Operation Overlapping," IEEE trans. Syst. Man, Cyber. A, Vol. 27, pp. 116-126, Jan. 1997.

김희완

1987년 광운대학교 전자계산학과 졸업(이학사).
1988년 한국전력공사 정보처리처(DBA)
1995년 성균관대학교 정보공학과(공학석사)
1996년 정보처리 기술사(정보관리 부문) 취득
1999년 정보시스템 감리인(한국전산원) 자격 취득
2002년 성균관대학교 전기전자 및 컴퓨터공학부(공학박사)
1996년 삼육의명대학교 전산정보과 조교수
2001년 삼육대학교 컴퓨터과학과 조교수
관심분야 : 컴퓨터 및 네트워크 보안, 동시성 제어, 분산 DB, 보안 시뮬레이션

서희석

2000. 2. 성균관대학교 산업공학과 졸업 (공학사).
2002. 2. 성균관대학교 전기전자 및 컴퓨터공학부 졸업 (공학석사).
2002. 3. ~ 현재 성균관대학교 정보통신공학부 박사과정 재학 중.
관심분야 : 네트워크 보안 시뮬레이션, 지능형 시스템, 분산 에이전트.