계약망 프로토콜을 적용한 보안 모델에서 에이전트 선택을 위한 퍼지 컨트롤러의 설계

이진아*, 조대호*

Design of Fuzzy-Controller for Agent Selection in CNP-applied Security Models

Jin Ah Lee, Tae Ho Cho

Abstract

광범위한 네트워크의 연결과 이를 이용하는 조직이나 개인의 증가로 인터넷은 정보를 교환하고 거래를 수행하는 주요한 수단이 된 반면에 해커나 바이러스의 침입 또한 증가하여 공격에 쉽게 노출되어있다. 이러한 보안상의 문제점을 해결하기 위하여 컴퓨터나 네트워크 시스템의 활동을 감시할 수 있는 침입 탐지 시스템(IDS)과 같은 보안 요소를 도입하였으며, 탐지에 대한 성능을 향상시키기 위하여 네트워크를 기반으로 하는 다중 침입 탐지 시스템을 응용하여 네트워크에 분산된 에이전트들 중에서 발생된 침입에 알맞은 에이전트를 선택하도록 하여 침입 탐지를 효과적으로 할 수 있게 하였다. 본 연구에서는 보안 시스템의 연동을 위하여 계약망 프로토콜을 적용하였다. 계약망 프로토콜은 분산된 에이전트들 중에서 입찰과정을 통하여 최상의 에이전트를 선택하는데 이때, 에이전트를 선택하는 과정에 있어서 퍼지 규칙 기반 시스템을 적용한 퍼지 컨트롤러를 설계하여 시뮬레이션 한다.

Key Words: Intrusion Detection System, Contract Net Protocol, Fuzzy Rule-based System

* 성균관대학교 컴퓨터공학과

1. 서론

컴퓨터 기술의 발달과 인터넷의 발전은 업무 효율을 향상시키고 생활의 질을 높여주는 등의 긍정적인 효과를 가져온 반면, 네트워크의 확장으로 외부에서의 시스템 불법 침입, 중요 정보의 유출 및 변경, 훼손, 불법적인 사용, 컴퓨터 바이러스 등의 역기능들이 증가되어 그 피해가 심각한 수준에 이르렀다[1]. 따라서 이러한 공격에 대한 대응책으로 현재 여러 보안 시스템들이 사용되고 있으며, 본 연구에서는 침입 탐지 시스템(IDS)을 보안 요소로 도입하였다.

침입 탐지 시스템은 네트워크 시스템이나 컴퓨터상에서 발생하는 이벤트들을 모니터링하고, 자료를 수집한 후 분석하여 침입 발생 여부를 탐지(detection)하고 대응(response)하는 행동을 취하는 자동화된 보안 솔루션이다.

네트워크 기반(network-based) IDS는, 시스템 내부에 설치되어 하나의 시스템 내부 사용자들의 활동을 감시하고 공격 시도를 탐지해 내는 호스트 기반(host-based) IDS와는 달리, 네트워크 상의 패킷을 분석하여 전체 네트워크에 대한 침입 탐지가 가능하게 하며, 호스트 기반의 IDS에서는 탐지 불가능한 침입도 탐지할 수 있다. 반면, 네트워크 기반 IDS는 많은 부하가 걸린 세그먼트들을 완전하게 처리할 수 없으며, 최근의 고부하 네트워크 환경에서는 패킷이 탐지되기도 전에 유실될 가능성이 높다는 단점이 있다.

따라서 본 연구에서는 네트워크를 기반으로 하는 다중 침입 탐지 시스템을 도입하였다. 분산 에이전트 기반의 침입 탐지 시스템은 침입 탐지를 다수의 분산 에이전트들이 나누어 수행하므로 시스템의 부하를 감소시키고 침입 탐지의 속도를 향상시키며 발생된 침입에 적당한 에이전트를 선택하여 침입 탐지의 성능을 향상시킬 수 있다. 이러한 다중 에이전트 환경에서 에이전트 사이의 연동에 있어 효율적인 수행 능력을 위해서는 분산된 에이전트들에게 효과적인 작업의 할당이 이루어져야 하며[2], 본 논문에서는 이러한 에이전트 사이의 연동을 위하여 계약망 프로토콜(Contract Net Protocol)을 적용하였다.

계약망 프로토콜은 분산된 에이전트들 중에 입찰(bidding)을 통해 최상의 에이전트를 선택하고 선택된 에이전트는 서비스를 제공하게 된다[3-5].

본 연구에서는 각 에이전트들이 입찰을 했을 때, 에이전트를 선택하는 커맨드 콘솔에서 선택 알고리즘을 이용하여 에이전트를 선택했을 때와 비교하여 퍼지 규칙 기반 시스템(Fuzzy Rule-Based System)을 적용하여 에이전트를 선택했을 때, 어떻게 작업이 할당되는지를 시뮬레이션 하여 비교하였다.

2. 배경이론 및 관련 연구

2.1 침입 탐지 시스템(IDS)

침입 탐지 시스템은 외부의 침입에 대해 능동적으로 대처 하는 시스템으로 방화벽의 앞 또는 뒤에서 침입 사실을 탐지해 침입자의 공격에 대응하기 위한 솔루션이다[6,7].

침입 탐지 접근 방법은 크게 오용(misuse) 탐지와 비정상(anomaly) 행위 탐지 방법으로 나눌 수 있다. 오용 탐지 방법은 일반적으로 침입이라고 알려져 있는 행위 또는 비정상적인 행위를 패턴으로 저장해 놓고, 이에 일치 또는 유사한 사용자의 행위가 나타났을 때 이를 탐지하는 것이다. 비정상 행위 탐지 방법은 시스템이나 네트워크에서 일어나는 행위들 중 일반적이지 않고, 발생 빈도가 매우 낮은 행위의 발생을 탐지하는 방법이다. 이러한 탐지 방법은 침입자의 행위가 일반 사용자의 행위와 주목할 만큼 다르다는 가정을 기반으로 한다.

2.2 계약망 프로토콜(Contract Net Protocol)

다중 에이전트 시스템에서 에이전트들은 시스템이 보다 나은 목표 달성을 위해 상호작용을 하고 에이전트들 사이의 상호작용들이 서로 조화될 수 있도록 대화(communication)하고 협력(cooperation)하 타협(negotiation)하는데, 에이전트들이 자원 경쟁을 줄이고, 교착상태를 피하며, 안전성을 유지할 수 있도록 조정하는 것이 중요하다[8].

이러한 다중 에이전트 시스템의 조정기법에는 일련의 메시지를 교환하는 프로토콜이

필요한데, 그 중 계약망 프로토콜은 분산된 문제(distributed problem)를 해결하는데 있어 에이전트들 사이의 통신을 하기 위한 도구중 하나로서 제안되었다[4].

계약망 프로토콜은 에이전트들이 계약에 의하여 분산된 문제를 해결하기 위하여 협상하고 통신하는 메커니즘을 제공한다[3]. 커맨드 콘솔은 에이전트들에게 수행될 필요가 있는 작업을 알리고, 에이전트들은 공지된 작업들을 수행하기 위해 bid를 만들어서 보내면 관리자는 에이전트들이 제출한 bid를 평가하여 최상의 에이전트를 선택하여 계약을 체결하게 된다[4,5].

2.3 계약망 프로토콜을 통한 연동

2.3.1. 계약망 프로토콜의 동작

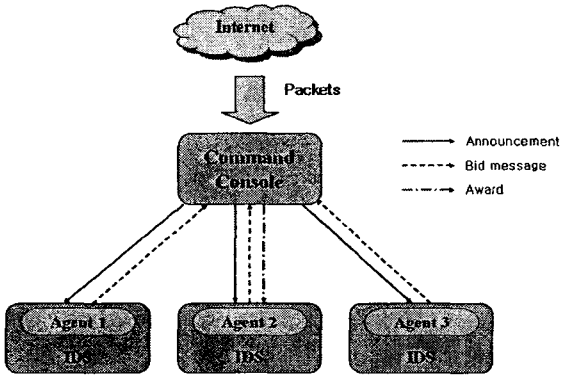

그림 1. 계약망 프로토콜의 연동 구조

먼저 내부 네트워크로 패킷이 유입되면 커맨드 콘솔은 모든 침입 탐지 에이전트들에게 입찰을 위한 메시지를 브로드캐스트 하게 된다. 이 메시지를 받은 에이전트들은 커맨드 콘솔에게 bid 메시지를 보내게 되고, 이 bid메시지를 가지고 선택 알고리즘에 의해 침입을 탐지할 에이전트가 선택되고 선택된 에이전트에게 award 메시지와 함께 패킷 정보를 담은 데이터를 보내게 되면, 선택된 에이전트는 이 데이터를 가지고 침입을 탐지 하게 된다.

2.3.2 에이전트 선택 알고리즘

커맨드 콘솔에서 어떤 에이전트를 선택할 것인가가 본 연구에서 중요한 부분인데 기존의 연구[9]에서는 각 에이전트가 bid 데이터의 loading 필드의 값이 임계값을 넘지 않은 경우에 bid 메시지를 중앙 콘솔에 보내게 되는데 우선적으로 expertise 필드의 값을 기준으로 정렬하여 가장 큰 값을 갖는 에이전트를 선택한다.

```
Let bidi be bids
Set bid_list = empty set
Let bid_list = ( bid1, bid2..., bid n ) be a list of bids
for i = 1 to n
  if loading of bidi >= threshold value
    Delete bidi from bid_list
Sort bid_list by expertise in descending order
if the number of bid including the greatest value of expertise >= 2 then
{
  Delete bids from bid_list except bids including the greatest value of expertise
  Sort bid_list including bids of the same expertise by experience in descending order
  if the number of bid including the greatest value of experience >= 2 then
  {
    Delete bids from bid_list except bids including the greatest value of experience
    Sort bid_list including bids of the same experience by loading in ascending order
  }
}
Select agent from bid_list(the first element)
```

그림 2. 기존 연구의 선택 알고리즘

만약 expertise의 값이 같은 에이전트가 존재하면 그 에이전트 중에 experience 필드의 값을 기준으로 다시 정렬하여 역시 가장 큰 값을 가진 에이전트를 선택한다. 여기서, experience 값마저 같은 에이전트가 존재한다면 마지막으로 loading 필드의 값을 기준으로 정렬하여 가장 작은 값을 가진 에이전트를 선택하게 된다.

3. 퍼지 컨트롤러의 설계

3.1. 퍼지 컨트롤러의 제안 및 구성

최근에는 웹 서버에 대한 공격보다는 침입 탐지 시스템 자체에 대한 공격이 더 많아졌다. 간단하고 단순한 공격 패킷들을 무수히 많이 보냄으로써, 탐지하고 대응하는 과정을 반복하게 하여, 실제로 중요한 공격에는 대처하지 못하게 하는 것이다. 따라서 대량의 트래픽에서 침입이 발생할 때, 이를 얼마나 효율적으로 탐지할 수 있는가가 침입 탐지 시스템의 성능을 측정하기 위한 중요한 요인이 된다. 이러한 문제를 해결하기 위해서는 다수의 IDS가 트래픽을 공유하도록 하는 것이 중요하다.

본 연구에서는 기존의 에이전트 선택에 있어서 전문성에 따라 한 에이전트로 작업이 편

중되는 한계를 갖는 것을 극복하기 위한 퍼지 컨트롤러를 제안하였다.

에이전트 선택을 위한 퍼지 컨트롤러는 퍼지 규칙 기반 시스템(Fuzzy Rule-based System)으로 구성되는데[10], 입찰한 에이전트의 전문성(Expertise)과 침입 상태(Intrusion State), 그리고 부하(Load)를 입력으로 퍼지 추론을 수행하여, 능력(Capability)을 출력한다.

시스템의 입출력에 대한 멤버십 함수(Membership Function)는 그림 3과 같다.

본 시스템은 총 36개의 퍼지 IF THEN 규칙(그림 4)을 사용하며, 실험에서는 네트워크 IDS의 수를 3개로 한정하고, 동일 시드에서 10,000개의 패킷을 발생시켜, 퍼지 컨트롤러를 적용한 경우와 기존의 선택 알고리즘을 사용하였을 때를 비교하였다.

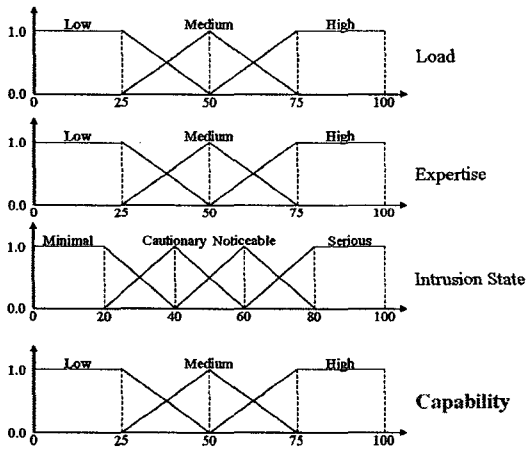

그림 3. 입출력에 대한 멤버십 함수

Rule 13:
IF *Loading=Low* ∧ *Expertise=Medium* ∧ *IS=Cautionary*
THEN *Capability=Low*
Rule 14:
IF *Loading=Medium* ∧ *Expertise=Medium* ∧ *IS=Cautionary*
THEN *Capability=Medium*
Rule 15:
IF *Loading=High* ∧ *Expertise=Medium* ∧ *IS=Cautionary*
THEN *Capability=Medium*
Rule 16:
IF *Loading=Low* ∧ *Expertise=High* ∧ *IS=Cautionary*
THEN *Capability=Medium*

그림 4. Fuzzy Rules

3.2 실험 결과

본 연구에서는 에이전트의 전문성을 달리하며, 모든 조합에 대하여 퍼지를 적용하였을 때와 적용하지 않았을 때를 비교하였다.

먼저 그림 5 와 같이 전문성이 서로 다른 에이전트들이 입찰했을 때, 퍼지 규칙기반 시스템을 사용하지 않는다면 부하가 임계값을 넘지 않을 시를 제외하고는 전문성이 높은 한 개의 에이전트로 전부 award되는 데에 반해, 퍼지를 적용하면, 침입 상태나 전문성을 고려하여 다른 에이전트들로 골고루 분산 되는 것을 볼 수 있다.

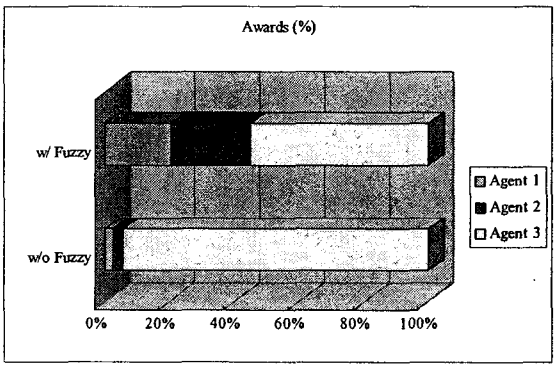

그림 5. 전문성이 서로 다른 에이전트가 입찰했을 때의 awards의 비율

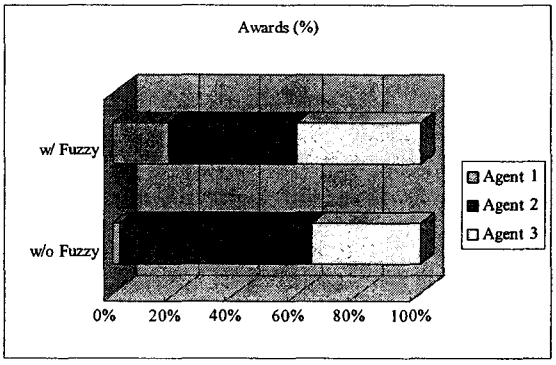

그림 6. 전문성이 같은 두 에이전트가 입찰했을 때의 awards의 비율

그림 6은 전문성이 높은 두개의 에이전트와 보통인 한 개의 에이전트가 있을 때를 시뮬레이션 하였을 때 awards의 비율을 나타낸다. 결과와 같이 퍼지를 적용하기 전에는 전문성이 같은 에이전트가 있다면 침입 상태에

따라서 침입을 받지 않고 있는 에이전트에게로 awards가 편중되는 현상이 발생하게 된다. 그러나 퍼지를 적용한 후에는 한 에이전트로 부하가 몰리는 것을 막고, 비록 전문성이 좀 낮더라 하더라도 침입상태와 부하를 고려하여 에이전트가 선택되는 것을 알 수 있다.

4. 결론 및 향후 연구

실험 결과에서 알 수 있듯이 퍼지 규칙 기반 시스템을 적용하였을 때 에이전트들 사이에 작업의 분산이 잘 이루어지는 것을 알 수 있으며, 기존의 커맨드 콘솔과는 달리 에이전트의 전문성, 침입 상태, 부하를 전체적으로 고려하여 효율적으로 에이전트를 선택할 수 있었다. 만약 전문성이 다른 에이전트로 구성되어있는 경우 부하가 전문성이 높은 에이전트로 편향되는 현상을 방지할 수 있으며, 전문성이 동일한 에이전트로 구성되어 있는 경우에도 기존보다 더 나은 로드 밸런싱 기능을 수행하는 것을 확인하였으며, 오판율(False rate)이 낮아지고, 침입 탐지 시간도 빨라질 것이라는 것을 기대할 수 있었다.

네트워크 기반의 침입 탐지 시스템에서 무엇보다도 중요한 것이 시스템의 부하라고 할 수 있으며, 로드 밸런싱이 최근의 고부하의 비대칭 스위치드 네트워크에서 중요한 이슈가 되고 있다. 또한 계약망 프로토콜이 메시지 기반의 프로토콜이기 때문에 갖는 한계가 바로 네트워크의 부하인데, 기존의 선택 알고리즘은 한 에이전트로의 부하를 더욱 가중시켜, 침입 탐지 시스템 자체를 공격하는 공격 시에는 더욱 취약하였다.

따라서, 향후 연구 과제로 본 연구를 발전시켜 전체 대상 네트워크를 구성하고, 구성된 네트워크 안에서 퍼지 컨트롤러를 사용하였을 때, 결과적으로 침입 탐지 성능이 어느 정도 향상 될 것인지를 시뮬레이션 하여야 할 것이다.

참고문헌

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

[2] K. M. Sim, S. K. Shiu, and B. L. Martin, "Simulation of a Multi-agent Protocol for Task Allocation in Cooperative Design," Proc. of IEEE SMC '99 Int'l Conf., vol. 3, pp. 95-100, 1999.

[3] J. Yang *et al.* "Coordination of Distrbuted Knowledge Networks Using Contract Net Protocol," Information Technology Conf., IEEE, pp. 71-74, 1998.

[4] 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.

[5] H. D. Parunak, "Manufacturing Experience with the Contract Net," In Research Notes in Artificial Intelligence: Distributed Artificial Intelligence, vol. 1, pp. 285-310, Morgan Kaufmann 1987.

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

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

[8] K. J. Suh, and T. H. Cho, "Application of Contract Net Protocol to the Design and Simulation of Network Security Model," Int'l Conf. of Korea Intelligent Information System Society, pp. 197-206, 2003.

[9] J. Yen and R. Langari, "Fuzzy Logic ; Intelligence, Control, and Information", Prentice Hall, 1999.

[10] J. Yen and R. Langari, "Fuzzy Logic ; Intelligence, Control, and Information", Prentice Hall, 1999.