계약망 프로토콜을 적용한 네트워크 보안 모델의 설계

서경진, 조대호

경기도 수원시 장안구 천천동 300 성균관대학교 정보통신공학부

Design of Network Security Model using Contract Net Protocol

Suh, Kyong Jin and Cho, Tae Ho

Sungkyunkwan University

요 약

최근에 분산 시스템과 같이 이기종의 컴퓨팅 환경을 효율적으로 통합하는 방법에 관한 다양한 연구가 진행되고 있다. 네트워크 보안에서는 각 보안 시스템들이 효율적인 침입탐지와 차단을 위해서 분산화되고 있으며 분산된 보안 시스템들을 조정하고 통합하기 위해서 분산인공지능(Distributed Artificial Intelligence)의 개념을 도입하고 있다. 본 논문에서는 분산침입탐지 시스템(Distributed Intrusion Detection System)과 침입차단 시스템(firewall)이 계약망 프로토콜(Contract Net Protocol)에 의해 상호 연동하여 외부 네트워크에서 유입된 패킷의 정보를 통해 침입을 탐지하고 차단하는 네트워크 보안 모델을 설계하였다. 본 연구진이 구성하고 있는 시뮬레이션 환경에서는 네트워크에 존재하는 다양한 보안 모델들을 계층적으로 구성하기 위해 DEVS 방법론을 사용하였다. 보안 시스템의 연동은 계약망 프로토콜에 의해 이루어지는데 네트워크에 분산되어 있는 각각의 전문성을 가진 침입탐지 에이전트들이 중앙 콘솔에 비드(bid)를 제출하고 중앙 콘솔은 최상의 비드를 제출한 에이전트를 선택하여 침입을 탐지하게 된다. 그리고 탐지된 정보를 참조하여 침입차단 시스템은 능동적으로 침입을 차단하게 된다. 이와 같은 모델의 설계를 통해서 기존의 침입탐지 시스템들이 탐지하지 못한 침입을 탐지하게 되고 보안시스템에서의 오류발생빈도를 감소시키며 탐지의 속도를 향상시킬 수 있다.

1. 서 론

침입탐지의 초기에는 네트워크에 단일침입탐지 시스템을 설치하여 네트워크를 감시하도록 하였다. 단일침입탐지 시스템의 사용은 상대적으로 시스템의 부하가 커져서 성능의 저하를 가져왔고 단일침입탐지 시스템이 한정된 규칙만을 가지고 침입을 탐지하기 때문에 새로운 침입을 탐지하는데 많은 문제점이 발생되었다. 이와 같은 문제점들을 보완하고 탐지에 대한 성능을 향상시키기 위해서 다중

침입탐지 시스템을 도입하게 되었다. 무엇보다도 다중침입탐지 시스템에서는 침입을 탐지하는 에이전트들의 연동이 시스템의 성능을 높이기 위한 중요한 요소이다. 따라서 에이전트에 근거한 연동을 설계하는데 있어서 높은 수행능력을 성취하기 위해서는 분산된 에이전트에게 효과적인 작업의 할당이 이루어져야 한다[1]. 이러한 이유로 인공지능과 자동제어(Automation Control)에 근거한 IC(Intelligent Control)가 필요하게 되었고 인공지능의 모든 분야의 아이디어와 연구결과가 문제영역을 조정하기 위해 적용되었으며 IC의 각 부문에서 Expert System Control, Fuzzy Control, Neural Network Control 그리고 Simulating Human Intelligent Control 등과 같은 시스템들이 나타났다[2]. 특별히 다중 에이전트 시스템에서는 분산인공지능의 새로운 기술에 대한 연구가 인공지능의 연구에서 중요한 분야가 되고 있다[3]. 본 연구에서 침입탐지 에이전트들이 문제를 해결하는 동안 상호 연동하기 위해 계약망 프로토콜이 적용되었다.

2. 시뮬레이션 환경설계

2.1 대상 네트워크의 SES

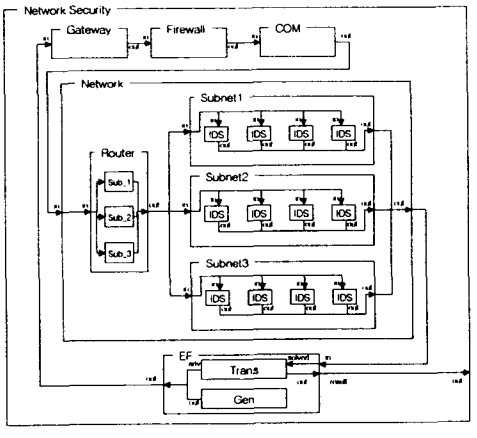

그림 1. DEVS 시뮬레이션 모델의 구조도

SES (System Entity Structure)는 계층적인 모델을 구성하고 설계된 모델에 근거하여 재사용을 위해 조직화하는 역할을 한다[4].

그림 2는 그림 1의 대상 네트워크를 SES 형식론을 사용하여 표현한 것이다. Network Security 모델은 Gateway, Firewall, COM, Network 그리고 EF 모델과 decomposition 관계를 가진다. Firewall 모델의 Outbound_Filter 모델은 Protocol, Address, Port 그리고 Data 모델과 specialization 관계를 가진다. 나머지 다른 모든 모델들도 계층적으로 decomposition이나 specialization 관계를 갖는다.

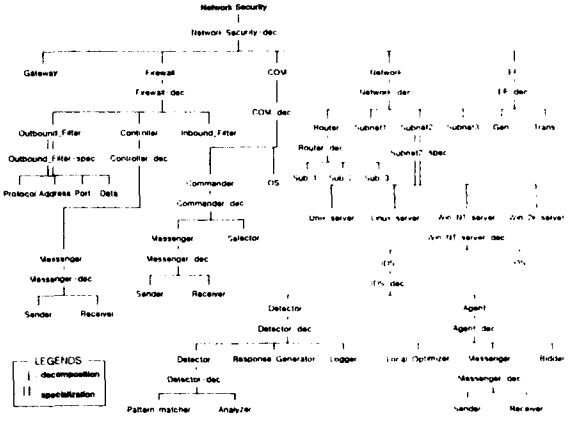

그림 2. 대상 네트워크의 SES

3. IDS 모델

3.1 IDS 모델의 구조 및 기능

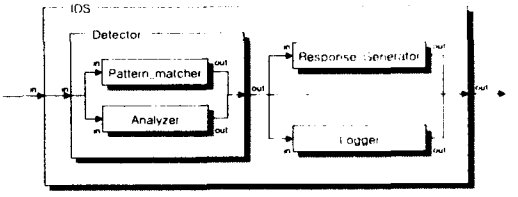

그림 3. IDS 모델의 구조

IDS 모델은 실질적으로 침입을 탐지하는 모듈로서 Detector, Response_Generator 그리고 Logger 모델로 구성된다.

3.1.1 Detector 모델

Detector 모델은 Pattern_matcher와 Analyzer 모

델로 구성되는데 기능은 다음과 같다.

Pattern_matcher는 데이터마이닝이나 data fusion 등을 사용해서 구성된 규칙에 의해서 침입이 발생했는지, 발생할 것인지를 결정한다[5]. 제안한 모델에서는 패킷 정보를 규칙과 비교하여 침입을 탐지하게 된다.[6] 예를 들면 Smurf 공격은 다음과 같이 표현될 수 있다.

icmp number(receive()) >= m and addr() = (host, broadcast).

Smurf 공격은 대상 호스트에서 목적지 주소가 브로드캐스트 주소와 같은 패킷의 개수가 임계값을 초과하는 것을 의미한다.

Analyzer는 호스트에 근거한 상태전이분석을 통해 침입을 탐지하게 된다. 이 모델은 시작상태에서 침입을 탐지할 때까지 하나 이상의 중간상태를 사용한다. 시작상태 이후에 key action에 의해 다음 상태로 인식되는데 여기서 인식된 action을 signature action이라고 한다. 침입은 일련의 signature action인 공격 시나리오에 따라 이루어진다. 따라서 signature action에 근거한 규칙을 통해서 침입을 탐지하게 된다.

3.1.2 Response_Generator 모델

이 모델은 침입을 탐지한 후 침입에 대한 response를 생성한다. 예를 들면 경보를 울리거나 report를 생성할 수도 있고 능동적으로 침입차단 시스템을 통해 패킷을 차단할 수도 있다.

3.1.3 Logger 모델

Detector 모델에 의해 침입이 탐지되는 과정에 대한 정보를 로그파일에 기록한다.

4. 에이전트간의 연동

4.1 계약망 프로토콜 설계

계약망 프로토콜은 분산된 문제를 해결하는 것에 있어 통신하고 조정하기 위한 도구로서 제안되었다. 계약망 프로토콜의 사용은 분산감지 시스템과 분산전달 시스템을 위해서 시도되었다[7]. 계약망 프로토콜은 에이전트들이 계약(contract)에 의하여 분산된 문제를 해결하기 위해서 협상하고 통신하는 메커니즘을 제공한다[8]. 에이전트들은 수행될 필요가 있는 작업을 알리고 다른 에이전트들에 의해 공지된 작업들을 수행하기 위해 비드를 만들고, 중앙 콘솔은 각 에이전트들이 제출한 비드를 평가해서 계약을 체결한다.

4.1.1 계약망 프로토콜의 구조

계약망 프로토콜은 모듈화와 객체지향설계에 근거한다. 침입탐지 에이전트 모듈은 도메인에 독립적인 모듈과 도메인에 의존적인 모듈로 구성되는데 도메인에 독립적인 모듈에는 중앙 콘솔(Command Console), Messenger, 그리고 Bidder가 있고 도메인에 의존적인 모듈은 응용 프로그램에 의존적인 함수들을 호출하는 Local Optimizer 모듈과 친밀하게 작동한다. 그림 4와 그림 5는 계약망 프로토콜의 구조와 에이전트의 구조를 나타내며 각 모듈들은 다음과 같이 동작한다.

중앙 콘솔은 에이전트의 위치에 대한 정보를 가지고 있으며 모든 에이전트를 중앙에서 통제한다. Messenger는 에이전트들 사이에 메시지를 보내고 받는 것을 관리한다. 중앙 콘솔에서 선택된 에이전트로서 award 메시지를 받아들이며 announcement 메시지를 중앙 콘솔에 보낸다. 에이전트의 위치를 알기 위해 중앙 콘솔에 query한다. Bidder는 수신한 announcement에 대한 응답으로 Local Optimizer로부터 에이전트의 상태정보를 받아서 중앙 콘솔에 제출할 비드를 만든다. 비드를 만들 때는 시스템 부하를 고려한다. Local Optimizer는 비드의 정보가 되는 시스템 정보를 계산하고 상태에 따라 갱신된 최신의 정보를 유지한다.

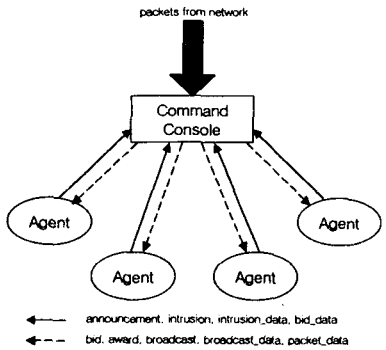

그림 4. 계약망 프로토콜의 구조 및 자료의 흐름

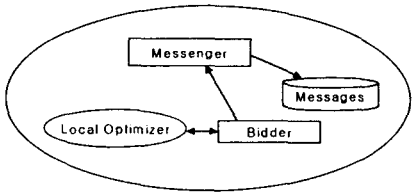

그림 5. 에이전트의 구조

4.1.2 메시지의 종류 및 구조

중앙 콘솔과 침입탐지 및 침입차단 에이전트들은 모두 Messenger 모델을 가지고 있는데 이 모델은 메시지의 송신과 수신을 담당한다. 메시지의 종류는 크게 컨트롤 메시지(control message)와 데이터 메시지(data message)가 있다. 컨트롤 메시지에는 다음의 다섯 가지가 있다.

Bid 메시지는 비드를 제출하도록 모든 침입탐지 에이전트에게 알린다. Award 메시지는 중앙 콘솔에서 선택된 에이전트에게 침입탐지 에이전트로 선택된 것을 알린다. Intrusion 메시지는 침입이 발생하거나 상태전이가 이루어지면 침입탐지 에이전트가 중앙 콘솔에 알린다. Intrusion 메시지를 받은 중앙 콘솔은 침입차단 시스템에 알려서 침입에 대처하게 된다. Announcement 메시지는 에이전트에서 침입을 탐지할 수 없는 상황이 되거나 상태전이로 에이전트 선택을 다시 해야 할 경우 중앙 콘솔에 알린다. Broadcast 메시지는 침입탐지 에이전트가 침입을 탐지하면 탐지에 대한 정보를 받은 중앙 콘솔이 모든 침입탐지 에이전트에 탐지정보를 보낸다는 것을 알린다.

메시지의 종류는 msg_type 필드의 값에 의해 판단한다. 메시지의 구조는 다음과 같다.

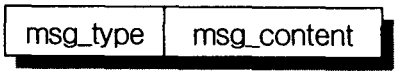

그림 6. 메시지의 구조

표 1. 메시지의 종류

msg_type	메시지 종류
0	Broadcast
1	Announcement
2	Bid
3	Award
4	Intrusion

데이터 메시지는 네 가지가 있는데 첫 번째로 bid_data는 그림 7과 같이 네 가지 필드로 구성된다. address는 비드를 보내는 에이전트의 주소를 나타내고 expertise는 각 에이전트가 탐지할 수 있는 규칙과 전문성을 수치화한 값이며 experience는 전에 탐지한 경험이 있는 침입에 대한 것을 수치화한 값이다. 그리고 loading은 침입탐지 시스템을 장착한 시스템의 CPU에 대한 부하를 수치화한 값이다.

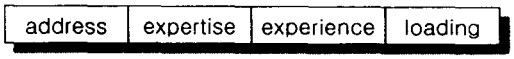

그림 7. bid_data 메시지의 구조

다른 데이터 메시지로 intrusion_data는 침입을 탐지하게 된 패킷의 정보를 가지고 있고 packet_data는 네트워크로 유입되는 패킷의 정보를 가지고 있다. 마지막으로 broadcast_data는 탐지된 침입에 관련된 정보를 포함한다.

4.3 침입탐지 에이전트의 선택과 연동

4.3.1 선택 알고리즘

각 에이전트는 loading 필드의 값이 임계값을 넘지 않은 경우에 bid_data를 중앙 콘솔에 보내게 되

는데 첫 번째로 expertise 필드의 값을 기준으로 정렬하여 가장 큰 값을 갖는 에이전트를 선택한다. 만약 같은 값을 갖는 에이전트가 존재하면 그 에이전트 중에 experience 필드의 값을 기준으로 다시 정렬하여 역시 가장 큰 값을 가진 에이전트를 선택한다. 만약 experience 값마저 같은 에이전트가 존재한다면 마지막으로 loading 필드의 값을 기준으로 정렬하여 가장 작은 값을 가진 에이전트를 선택하게 된다. 다음은 에이전트 선택 알고리즘이다.

Let bid_i be bids

Let bid list (bid_1, bid_2,……, bid_n) be a list of bids

Set bid list ∅

Sort bid list by expertise in descending order

if the number of bid including the greatest value of expertise > 2 ther

{

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)

4.3.2 선택 및 연동과정

시뮬레이션이 시작되면 중앙 콘솔은 모든 침입탐지 에이전트에게 bid 메시지를 보내고 이 메시지를 받은 에이전트들은 bid_data 메시지를 보낸다. 중앙 콘솔은 bid_data를 가지고 선택 알고리즘에 의해 침입을 탐지할 에이전트를 선택하게 되고 선택된 에이전트에게 award 메시지를 보낸다. award 메시지를 받은 에이전트는 packet_data를 기다리고 중앙 콘솔은 패킷 정보를 packet_data에 복사하여 선택된 에이전트에게 보낸다. 선택된 에이전트는 이 데이터를 가지고 침입을 탐지하게 된다.

침입탐지 과정 중 상태전이가 발생한 경우에 에이전트는 중앙 콘솔에 announcement 메시지를 보내고 이 메시지를 받은 중앙 콘솔은 위의 과정과 마찬가지고 bid 메시지를 보내고 에이전트 선택과정을 반복하게 된다.

침입을 탐지한 경우에는 선택된 에이전트가 intrusion 메시지를 중앙 콘솔에 보내고 intrusion_data 메시지를 보낸다. 이 메시지를 받고 중앙 콘솔은 침입차단 시스템에 intrusion, intrusion_data 메시지를 보낸다. 또한 중앙 콘솔은 broadcast 메시지와 침입에 대한 정보를 broadcast_data 메시지로 보낸다. 그런 다음 다시 bid 메시지를 보내고 위의 에이전트 선택과정을 반복한다.

5. 결론

계약망 프로토콜을 적용한 네트워크 보안 모델의 설계를 바탕으로 DEVS 방법론을 사용하여 시뮬레이션 환경을 구축하고 시뮬레이션을 실행함으로써 단일침입탐지 시스템 및 블랙보드를 사용한 다중침입탐지 시스템과 시뮬레이션 결과를 비교하여 각 시스템들의 특성을 파악할 수 있다. 시뮬레이션 결과를 평가하는 기준은 침입탐지시간과 오류(false positive or false negative)의 발생빈도가 될 수 있으며 특히 블랙보드와는 어느 시스템이 새로운 침입을 효과적으로 탐지할 수 있는지를 비교하여 연동의 효용성을 파악할 수 있다.

Acknowledgements

본 연구는 한국과학재단 목적기초연구(R05-2002-000-00107-0)지원으로 수행되었음.

참고문헌

[1] 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.

[2] Wang Junpu, Chen Hao, Xu Yang and Liu Shuhui, "An Architecture of Agent-Based Intelligent Control Systems," Proceedings of the 3rd World Congress on Intelligent Control and Automation, IEEE, June 28-July 2, pp. 404-407, 2000.

[3] Shungeng Hu, Li Zhang and Yixin Zhong, "Theories, Technology and Application of Multi-Agent Systems," Computer Science, Vol. 26, No.9, pp. 20-24, 1999.

[4] Bernard P. Zeigler, Herbert Praehofer and T.G. Kim, "Theory of Modeling and Simulation Second Edition: Integrating Discrete Event and Continuous Complex Dynamic Systems," Academic Press, 2001.

[5] Shan Zheng, Chen Peng, Xu Ying and Xu Ke, "A Network State Based Intrusion Detection Model," Computer Networks and Mobile Computing, 2001. Proceedings. International Conference on 2001, pp. 481-486, 2001.

[6] H.S. Seo and T.H. Cho, "Simulation of Network Security with Collaboration among IDS Models," Lecture Notes in Artificial Intelligence, Springer Verlag, Dec. 2001.

[7] T. Sandholm, "An Implementation of the Contract Net Protocol based on Marginal Cost Calculations," in 11th National Conference on Artificial Intelligence (AAAI-93), Washington. DC, 1993.

[8] 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.