제 19 회 한국정보처리학회 춘계학술발표대회 논문집 제 10 권 제 1 호 (2003. 5)

애드혹 네트워크에서 AODV 를 이용한 침입 탐지 방안

김경자, 홍성옥, 장태무
동국대학교 컴퓨터공학과
e-mail : sunaunt@hanmail.net

Intrusion Detection Scheme using AODV Protocol in Ad-Hoc Networks

Kyoung-Ja Kim, Sung-Ock Hong, Tae-Mu Chang
Dept. of Computer Engineering, Dong-Guk University

요 약

무선 애드 혹 네트워크에서의 침입 탐지 방안으로 호스트 기반 침입 탐지 시스템과 네트워크 기반의 침입 탐지 시스템의 기능을 포함하고 있는 에이전트를 두어서, 애드 혹 네트워크에 적합한 침입 탐지 방안을 제안하고자 한다. 애드 혹 네트워크에서의 라우팅 프로토콜인 AODV 프로토콜을 이용하여 침입 패턴을 공유한다. 또한 네트워크 상에 있는 노드들을 여러 개의 클러스터 단위로 나누어 지역화를 시킴으로써 침입 분석이나 탐지에 있어서 더욱 효율적으로 관리하고자 한다.

1. 서론

최근 침입 탐지 시스템(IDS: Intrusion Detection System)의 방화벽의 부족한 부분을 보강해 줄 수 있는 방안으로 침입 탐지 시스템이 많이 상용화되었다. IDS 는 네트워크나 호스트에서의 시스템에 대한 불법 행위나 공격 등을 탐지하여 대응 방안을 세울 수 있게 하는 역할을 한다.

또한, 기반 네트워크가 존재하지 않거나 이의 설치가 어려운 애드 혹 네트워크에서의 새로운 침입 감내 방안에 대해 많은 연구가 진행되어지고 있다.

따라서, 본 논문에서는 애드 혹 네트워크에서의 침입 탐지 방안으로서 애드 혹 네트워크의 라우팅 알고리즘인 AODV 와 CGSR 프로토콜을 응용한 침입 탐지 방안을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2 장은 관련 연구로서 기존의 침입 탐지 시스템을 분류하여 보고, 일반적인 애드 혹 네트워크에서의 노드의 이동성으로 인한 문제점을 알아본다. 3 장에서는 제안하고자 하는 시스템에서의 에이전트의 기능과 CGSR 을 응용하여 만든 노드들의 클러스터링 기법을 소개하고 있다. 4 장은 AODV 프로토콜을 응용하여 만든 침입 탐지 방안으로 정보 수집, 침입 분석 및 탐지 매카니즘과 침입 패턴에 대한 공유 방법을 보여준다. 마지막으로 5 장은 결론 및 앞으로의 향후 연구과제를 기술한다.

2. 관련 연구

본 논문에서는 애드 혹 네트워크에서의 에이전트를 기반으로 하는 침입 탐지의 새로운 방안을 제안하고자 한다. 애드 혹 라우팅 프로토콜인 AODV 를 기반으로 전체적인 침입 탐지 및 분석을 클러스터 내의 노드들이 공유하는 방안을 제안하다. 따라서 이 장에서는 침입 탐지 시스템의 분류를 보고, 기존의 무선 애드 혹 네트워크의 문제점을 알아보고자 한다.

2.1 IDS 의 분류

기존의 침입 탐지 기술을 탐지 모델별로 분류하면 오용 탐지(Misuse Detection)와 비정상 탐지(Anomaly Detection)로 분류 할 수 있다. 오용 탐지는 알려진 취약점에 대한 패턴을 보유하여 침입의 의혹이 있는 패턴에 대해서는 비교하여 정해진 모델과 일치하는 경우를 침입으로 간주한다. 구현 방법이 상대적으로 용

이하고 정확성이 높고, 알려진 침입에 대해서는 100% 탐지가 가능한 장점을 가지고 있다. 반면에 단점으로는 감사(Auditing)정보에 대한 의존도가 높고, 새로운 침입에 대해서는 취약점을 가지고 있으나, 현재 대부분의 사용 침입 탐지 시스템에서 사용하고 있다.

비정상 탐지(Misuse Detection)는 비정상적인 행위나 사용을 탐지하는 방식으로 정해진 모델을 벗어나는 경우를 침입으로 간주한다. 예상치 못한 취약점을 이용한 침입에 대한 탐지가 가능하고, 보안상의 취약점을 사용하지 않는 권한 남용형 공격 탐지가 가능하다는 장점을 가지고 있다. 반면, 주기적인 행동프로파일 재학습이 필요하고, 불완전한 정상행위 학습에 따른 높은 false-positive 오류 가능성이 있다. 또한 정상 행위 프로 파일 내에 침입 행위를 포함시킬 가능성이 있는 단점을 가지고 있다.[1]

또한, 침입 탐지 시스템을 호스트의 불법 액세스를 탐지하는데 초점을 맞춘 호스트 기반의 침입 탐지 시스템과 네트워크 공격을 탐지하는데 초점을 두는 네트워크 기반의 침입 탐지 시스템으로 분류할 수가 있다.

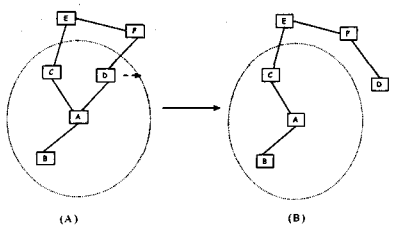
호스트 기반의 침입 탐지 시스템(Host-Based Intrusion Detection System)은 개별 호스트의 운영체제가 제공하는 보안 감사 로그, 시스템 로그, 사용자 계정들의 정보를 이용하여 호스트에 대한 공격을 탐지한다. 대부분의 HIDS 는 각 호스트에 상주하는 에이전트와 이들을 관리하는 에이전트 매니저로 구성된다. 특히, 불법적인 접근뿐만 아니라 합법적인 사용자에 의한 불법 행위도 탐지 할 수 있으므로 내부자에 의한 남용을 방지하거나 사후 추적을 가능하게 한다. 반면에, 상위 계층의 로깅 정보만을 해석하므로 네트워크의 공격 탐지는 거의 불가능하고, 보호하고자 하는 모든 호스트에 설치되어야 한다.

네트워크 기반의 침입 탐지 시스템(Network-Based Intrusion Detection System)은 네트워크 패킷이나 SNMP MIB, 응용 프로그램 로그 등을 분석하여 침입을 탐지한다. 네트워크 기반의 공격을 탐지하여 네트워크 기반 구조를 보호하고자 하는 것이 목적인 만큼 대부분의 경우 HIDS 에서처럼 특정 호스트의 공격은 탐지하거나 상세란 기록을 남길 수는 없다. 또한 Network-Based Monitor 들은 능동적으로 프로토콜에 관여하는 일이 없고, 단지 전송되는 패킷을 수동적으로 수집, 분석하는 만큼 공격자가 쉽게 액세스할 수가 없고 따라서 공격에 노출될 위험도 적다. [2]

2.2 애드 혹 네트워크의 노드 이동성

일반적으로 유선과 무선의 이동 네트워크에서 구조적인 면이나 행동적인 면에서의 차이점으로 인해 기존의 침입 탐지 시스템이 무선 애드 혹 네트워크에는 적합하지 않다.[1]

무선 애드 혹 네트워크에서의 네트워크 모니터링은 모든 네트워크 노드에서 수행된다. 그러나 무선 애드 혹은 노드의 이동성이 빈번하게 발생하므로 잦은 토폴로지의 변화가 발생한다. [그림 1]은 노드의 이동성에 의한 토폴로지의 변화를 보여준다.



[그림 1] 노드의 이동성으로 인한 토폴로지 변화

그림에서 보면, (a)는 원은 노드 A 의 범위를 보여준다. 노드 A 에서 노드 D 로의 연결이 있으나, 노드 D 가 노드 A 의 범위를 벗어나고자 하는 경우에는 (b)와 같이 변화하게 된다. 즉, 노드 A 에서 노드 D 로의 연결 경로는 A, C, E, F, D 로 변화하게 된다.

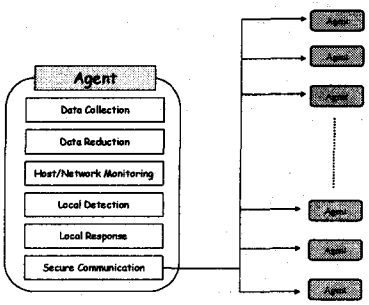
이와 같이 애드 혹 네트워크 경우는 노드의 이동성으로 인해 라우팅 정보가 자주 변화하게 된다. 이런 점을 고려한 방안으로 AODV 를 응용하여 침입을 탐지하고자 한다.**[3,4]**

3. 에이전트를 기반으로 하는 침입 탐지

최근에 침입 탐지 시스템에서 대두되고 있는 방안으로는 지능을 가지고 자율적으로 이동하면서 노드에 독립적으로 작업을 수행 할 수 있는 프로세스인 에이전트를 기반으로 탐지할 수 있는 방안이 연구되어지고 있다. 제안하고자 하는 탐지 방안도 애드 혹 네트워크에 적합할 수 있도록 여러 기능을 포함하고 있는 에이전트를 기반으로 한다.

3.1 AODV 침입 탐지의 구조

에이전트를 기반으로 하는 침입 탐지 시스템으로 각 노드의 기능을 호스트 기반과 네트워크 기반의 기능을 합한 하이브리드의 기능을 갖는 에이전트의 기능을 각 노드가 가지게 된다. 다음의 [그림 2]는 각 노드에 탑재되는 에이전트의 기능을 보여준다.



[그림 2] 에이전트의 기능

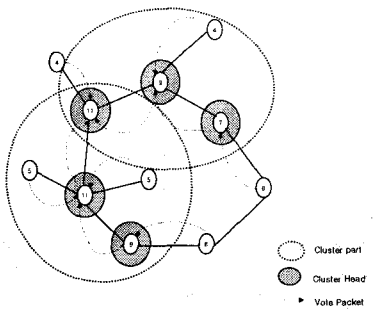
에이전트의 기능을 보면, 일반적으로 호스트 기반의

침입 탐지 시스템이 갖는 기능으로 데이터 수집, 데이터 축약, 모니터링, 탐지 및 응답의 기능을 포함하고, 네트워크 기반의 침입 탐지 시스템에서 갖는 네트워크 모니터링의 기능도 포함을 한다. 또한, 여러 에이전트들과의 안전한 통신을 위한 모듈이 추가된다. 네트워크 내에 있는 모든 노드들에게는 위의 기능을 모두 갖춘 에이전트를 탑재하고, 같은 클러스터 내에 있는 에이전트들끼리 침입에 대한 정보를 공유할 수 있도록 한다.

3.2 노드의 지역화

무선 애드 혹 네트워크에서는 노드의 이동성으로 인해 토폴로지가 자주 변화하게 된다. 따라서, 침입이 발생하여 복구가 필요한 경우에 토폴로지의 변화로 인해 복구가 불가능해 지는 경우가 발생할 수도 있다.

따라서, 본 논문에서는 애드 혹 네트워크상에 있는 많은 노드들을 몇 개의 클러스터 단위로 분리를 하여, 복구 시에 드는 전체적인 오버헤드를 줄일 수 있는 방안을 제안한다. [그림 3]은 노드들을 그룹화(클러스터링)하는 과정을 보여준다. 노드를 클러스터링 하는 방법으로는 무선 애드 혹 네트워크에서의 라우팅 프로토콜인 Clustered Gateway Switch Routing Protocol 을 응용하였다.[5,6]



[그림 3] 노드의 지역화

노드의 지역화 과정은 CGSR 에서 쓰이는 방법 중 싱글 홉 라우팅 통신을 적용하였다. 노드의 지역화 과정으로는 첫번째로 각 노드는 인접한 모든 노드들에게 자신에게 연결되어 있는 노드의 수를 브로드캐스팅한다. 두번째, 인접한 노드로부터 받은 연결 개수를 자신의 연결 개수와 합하여 다시 인접한 노드들에게 브로드캐스팅한다. 셋째, 각 노드는 인접한 노드들 중에 연결 개수의 값이 가장 큰 노드에게 Cluster head 를 위한 Vote 패킷을 보내게 된다.마지막 단계로는 Vote 패킷을 하나 이상 받은 노드는 클러스터 헤드로서 결정이 되고, 클러스터 헤드와 연결이 된 다른 노드들은 하나의 클러스터로 구성되어지게 된다.

그림에서 보는 바와 같이, 하나의 노드는 여러 클러스터에 중복되어 속할 수 있고, 같은 클러스터 내에 있는 노드들은 같은 침입 패턴을 공유하게 된다. 이렇게 많은 노드들을 몇 개의 클러스터 단위로 지역화를 시켜 클러스터 단위로 관리를 하게 된다. 즉 애드 혹 네트워크의 가장 큰 문제점인 잦은 토폴로지의 변화로 인한 문제점을 노드의 지역화로 인해 줄이고자 한다.

4. 침입 탐지 방안

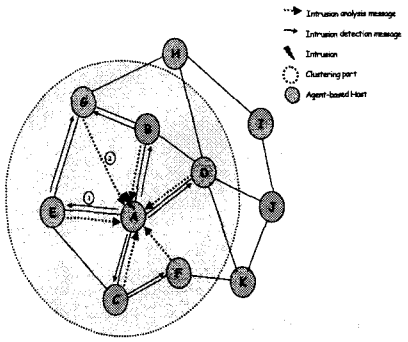
본 논문에서 제안하고자 하는 침입 탐지 방안으로는 각 노드의 에이전트가 모니터링을 하여 침입으로 의혹이 가는 데이터에 대해 같은 클러스터 내에 있는 다른 노드들과 협의를 하여 침입으로 간주하는 방식을 따른다.

4.1 정보 수집

일반적인 침입 탐지 시스템에서의 기본적으로 필요한 기술로서 정보 수집의 기술이 필요하다. 본 논문에서는 정보 수집의 기술로 기존의 시스템에서의 특정한 노드에서의 수집이 아니라, 에이전트를 탑재한 모든 노드들이 모니터링하여 데이터를 수집하게 된다. 여러 개의 클러스터 단위로 나뉘어진 노드들은 같은 클러스터 내의 노드들끼리 정보를 공유하게 된다. 여기서 정보를 수집하는 방법으로는 클러스터 헤드를 선출하는 방식처럼 각 노드가 모니터링한 결과를 클러스터 헤드에게 보내게 된다. 클러스터 헤드는 클러스터 내의 노드들에게서 보내 온 정보를 수집하여 침입으로 의혹이 가는 정보에 대해서는 클러스터 내의 다른 노드들에게 재전송하여 침입으로 간주할 지의 과정을 거치게 된다.

4.2 침입 분석 및 탐지

본 논문에서 침입을 분석하기 위해서 AODV 프로토콜을 응용하였다.[3] 다음의 [그림 4]는 침입을 분석하는 과정을 보이고 있다.



[그림 4] 침입 분석 및 탐지 과정

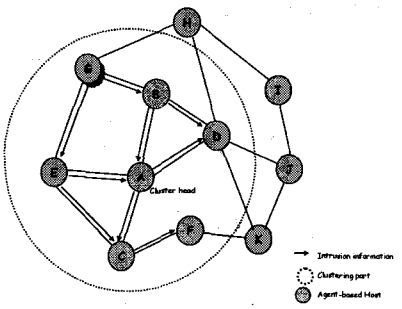
침입으로 간주가 되는 패턴이 생성되어, 침입으로 결정되는 과정으로는, 첫번째, 노드 A 에서 침입으로 간주되는 행동 패턴이 모니터링이 되면, 노드 A 는 인접한 노드 B, C, D, E 에게 새롭게 모니터링된 침입 패턴에 대해 전송하게 된다. 새로운 침입 패턴을 전송받은 노드 B, C, D, E 는 전송 받은 패턴을 각각 하위의 노드들에게 다시 전송하게 된다. 이러한 과정을 거쳐 클러스터 내의 모든 노드들이 새롭게 모니터링된

패턴을 전송 받을 수 있게 된다. 둘째, 새로운 패턴 메시지를 받은 노드들은 각각의 보유 정보를 통해 새로운 패턴이 침입으로 간주되는 지의 여부를 노드 A에게 Vote 패킷을 보내게 된다. 클러스터 내의 모든 노드들에게서 Vote 패킷을 받은 노드 A는 클러스터내의 노드들로부터 받은 Vote 패킷을 통해 새로운 패턴에 대해 침입으로 결정하게 된다. 셋째, 침입으로 결정이 되면 다시 한번 클러스터내의 모든 노드들에게 새로운 침입 패턴에 대한 정보를 재전송함으로써 클러스터 내의 모든 노드들이 네트워크 침입 패턴에 대해 같은 정보를 공유하게 된다.

4.3 침입 패턴 공유

제안한 논문에서의 침입 패턴 공유는 같은 클러스터 내의 모든 노드들이 각 노드에서 결정된 호스트 기반의 침입 탐지 패턴과 Voting 알고리즘을 통해 클러스터 헤드에서 결정된 네트워크 침입 패턴을 공유하게 된다. 하나의 노드가 여러 클러스터에 중복되어 포함될 수도 있으므로, 네트워크 전체로 보면 각 클러스터끼리의 정보 공유가 가능해지게 된다.

침입 패턴 공유를 위해서 각 노드가 보유하고 있는 침입 패턴에 대해서 On-Demand 형식의 AODV 방식으로 침입 패턴을 브로드캐스팅하게 된다. AODV 프로토콜 방식에 따라 각 노드는 클러스터 내의 인접한 노드의 정보를 가지고 있는 라우팅 테이블을 유지하고 있어야 한다. 각 노드가 유지하고 있는 라우팅 테이블에 따라 인접한 노드에게 자신의 정보를 전송 해줄 수 있다. 다음의 [그림 5]는 침입 패턴의 공유 과정을 보여준다. [6]



[그림 5] 침입 패턴의 공유 과정

클러스터 내의 모든 노드들은 침입에 대한 보유 정보가 변경 될 때마다 변경된 정보를 클러스터 내의 다른 노드들에게 전송하게 된다.

그림에서 보면, 노드 G가 변경된 정보에 대해 전송을 하고자 할 때, 노드 G는 자신의 보유한 라우팅 테이블에 따라 노드 B, E에게 새롭게 변경된 정보를 전송한다. 노드 B, E는 다시 노드 C, A, D에게 재전송한다. 노드 C, A, D는 하위의 다른 노드들에게 재전송하게 된다. 이런 과정을 거쳐, 클러스터 내의 모든 노드들이 같은 패턴을 공유하게 된다.

5. 결론 및 향후 연구 과제

본 논문에서는 애드 혹 네트워크에서의 라우팅 알고리즘인 Clustered Gateway Switch Routing Algorithm과 Ad-Hoc On-Demand Distance Vector Routing Algorithm을 응용하여, 네트워크내에 존재하는 많은 노드들을 여러 개의 클러스터 단위로 나누어서 관리의 효율을 높이고, 클러스터 내의 노드들끼리의 침입 패턴에 대한 공유를 하고자 한다. 기존의 유선의 네트워크망에 적용 가능한 침입 탐지 방안들이 무선의 애드 혹 네트워크망에는 부적합 하다고 보고 무선 애드 혹 네트워크에 적합한 침입 탐지 방안으로 에이전트를 기반으로 하는 방안을 제안하였다. 기존의 다른 방안과는 다르게 각 노드에 탑재된 에이전트가 호스트 모니터링과 네트워크 모니터링을 담당하고, 호스트 모니터링에 대해서는 각 노드에서 보유하고 있는 침입 패턴을 통해 침입으로 결정을 내리게 되고, 네트워크 모니터링을 통해 발견된 새로운 침입 패턴에 대해서는 같은 클러스터 내의 있는 모든 노드들이 공유할 수 있는 방안으로 클러스터 헤드에서의 Voting 방법을 적용하여 침입으로 결정하여 클러스터내의 모든 노드들이 새로운 침입 패턴에 대해 서로 공유할 수 있도록 하였다.

본 논문에서 제안한 방안이 기존의 이동 에이전트를 이용한 방안[1,2,7,8]보다도 효율적인 지에 대한 비교 분석에 대해서 향후에 연구할 예정이다. 또한, 각 노드에서의 모든 기능을 포함하고 있는 에이전트의 오버헤드를 줄일 수 있는 방안에 대해서도 모색해 보고자 한다.

참고문헌

[1] Yongguang Zhang and Wenke Lee, "Intrusion Detection in Wireless Ad-Hoc Networks", The Sixth Annual International Conference on Mobile Computing and Networking(MobiCom'2000), August, 2000.

[2] Oleg Kachirski and Ratan Guha, " Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks", IEEE Workshop on Knowledge Media Networking (KMN'02), July 2002.

[3] Lidong Zhou and Zygmunt h Hass, "Securing Ad Hoc Networks", IEEE Network, 1999.

[4] David B Johnson, "Routing in Ad Hoc Networks of Mobile Hosts", IEEE Workshop on Mobile Computing Systems and Applications, December 1994.

[5] E.M. Royer and C.K. Toh. "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks", IEEE Personal Communications Magazine, April 1999, pp. 46-55.

[6] Chales E.Perkins and Elizabeth M.Royer, "Ad-Hoc On-Demand Distance Vector Routing", Proceeding of MobiCom, 1999, pp 207-218.

[7] Farooq Anjum and Amjad Umar, " Agent Based Intrusion Tolerance Using Fragmentation Redundancy Scattering", IEEE, 2000.

[8] Yves Deswarte and Laurent Blain, "Intrusion Tolerance in Distributed Computing Systems", IEEE Symposium on Research in Security and Privacy, May, 1991.