무선 애드혹 네트워크 상에서의 침입 감내 방안

김경자° 홍성옥 장태무
동국대학교 컴퓨터공학과
sunaunt°@freechal.com jtm@dgu.ac.kr

Intrusion Tolerance Scheme in Wireless Ad-Hoc Networks

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

요 약

Ad Hoc망은 이동 호스트들로만 구성된 네트워크로서, 토폴로지의 작은 변화나 중앙 집중화 된 모니터링과 관리면에서의 기술 부족으로 인해 많은 취약점을 가지고 있다. 반면에 유선 네트워크에서 개발된 많은 침입 탐지 기술은 새로운 환경에서는 적절치가 않다. 따라서, 본 논문에서는 무선 Ad Hoc 네트워크상에서 이동 에이전트를 호스트 모니터링과 네트워크 모니터링의 기능을 분류하여 네트워크 망 내에서 연결된 개수에 따라 노드의 역할을 분담하여 침입을 감내 할 수 있는 방안을 제안하고자 한다.

1. 서 론

본 논문에서는 Ad Hoc 망에 적합한 침입 탐지 방안 및 침입 감내 방안을 이동 에이전트의 특성을 고려하여 제안하고자 한다. Ad Hoc망은 전형적인 무선 네트워킹과는 다른 새로운 무선 네트워킹 패러다임으로써 기존 유선 망의 하부 구조에 의존하지 않고 이동 호스트들로만 구성된 네트워크이다.

이동 Ad-hoc 네트워크는 다음과 같은 특성을 가지며, 이동 Ad-Hoc 네트워크를 위한 라우팅 프로토콜은 이와 같은 다양한 네트워크 특성을 고려하여 연구되어지고 있다. 첫째, 노드의 이동에 따라 네트워크 토폴로지가 동적으로 변환한다. 네트워크의 토폴로지의 변화는 빈번한 루트 정보의 갱신을 야기시켜 루트 정보의 관리를 복잡하게 하며, 이를 위한 라우팅 제어 메시지는 네트워크의 오버헤드로서 작용한다. 둘째, 이동 노드들은 무선 인터페이스를 사용하여 서로 통신한다. 무선 인터페이스는 기본적으로 전송 대역폭 및 전송 거리 상의 제약이 있다. 따라서, 원거리 노드들간의 통신을 위해서는 멀티 홉 통신이 필수적이다. 멀티 홉 통신을 위해 각 노드는 호스트 기능 외에 라우팅 기능도 포함되어 져야 한다. 셋째, 이동 노드들은 제한된 용량의 배터리를 사용하기 때문에 에너지 사용에 있어 제약이 크다. 따라서, 배터리 상태를 고려한 통신이 필요하다. 마지막으로 이동 노드들은 무선 인터페이스를 사용하여 서로 통신하고 있으며, 모든 노드들이 라우팅 기능을 가지고 있기 때문에 보안 상으로 매우 취약한 단점을 가지고 있다. 특히, 브로드 캐스팅 되는 라우팅 제어 메시지는 해킹의 위험이 크다[1].

본 논문에서는 이동 에이전트를 이용하여 침입 감내 방안을 제안한다. 여기서 이동 에이전트란 지능을 가지고 자율적으로 이동하면서 노드에 독립적으로 작업을 수행할 수 있는 프로세스를 말한다. 또한 이동 에이전트는 특정 노드의 상태에 영향을 받지 않으며, 통신 상태에 관계없이 작업을 수행할 수 있다. 이동 에이전트의 이점으로는 네트워크 트래픽 감소, 비동기적인 상호 작용, 부하 균형, 서비스의 분산 및 병렬 처리 등이 있다. 이러한 이동 에이전트의 특성을 고려하여 Ad Hoc 망 내의 노드들의 전체적인 부하 균형을 이룰 수 있다.

2. 관련 연구

기존의 네트워크 망 내에서의 침입 탐지 기술을 침입 모델을 기반으로 분류를 하면 비정상 탐지(Anomaly Detection)와 오용 탐지(Misuse Detection)로 구분할 수 있다. 비정상 탐지는 비정상 행위나 컴퓨터 자원의 사용을 탐지하여 정해진 모델을 벗어나는 경우를 침입으로 간주한다. 주기적인 행동 프로파일 재학습이 필요하고, 불완전한 정상행위 학습에 따른 높은 false-positive 오류 가능성이 있다. 반면에 새로운 공격의 자동적 발견이 가능하고, 운영체제에 덜 의존적이고 보안상의 취약점을 사용하지 않는 권한 남용형 공격 탐지도 가능하다는 장점을 가진다. 반면에, 오용 탐지는 시스템과 응용 프로그램의 취약점을 탐지하여 정해진 모델과 일치하는 경우를 침입으로 간주하는 방식으로 감사(Auditing)정보에 대한 의존도가 높고, 새로운 침입에 대해서는 취약한 점을 지닌다. 반면 장점으로는 구현 방법이 상대적으로 용이하고 정확성 또한 높고 알려진 침입에 대해서는 거의 100% 탐지가 가능하다.

침입 탐지 기술을 데이터 소스에 기반 하여 분류를 하면 호스트의 불법적인 침입을 탐지하는데 초점을 맞추는 호스트 기반 침입 탐지 시스템(Host-Based Intrusion

Detection System)과 네트워크 공격을 탐지하는 네트워크 기반의 침입 탐지 시스템(Network-Based Intrusion Detection System), 두 가지의 기능을 모두 갖춘 하이브리드 침입 탐지 시스템(Hybrid Intrusion System)으로 분류할 수 있다.

침입 탐지 시스템의 수행 과정을 살펴 보면, 첫 번째는 정보 수집(Data Collection)단계로 호스트 로그 정보, 멀티 호스트간 로그 정보, 네트워크 패킷 등을 수집한다. 두 번째로는 정보 가공 및 축약(Data Reduction)단계로 Raw 데이터로부터 의미 있는 정보로 가공한다. 세 번째는 침입 분석 및 탐지(Analysis & Detection)단계로 침입으로의 가부 판정을 한다. 마지막으로 보고 및 조치(Report & Response)단계로 세 번째 단계에서 침입으로 판정되면 즉각적으로 보고 및 해당 조치 사항을 바로 수행한다.

3. 제안한 침입 감내 방안

무선 애드혹 네트워크상에서의 이동 에이전트를 이용하여 침입을 어느 정도 감내 할 수 있는 방안을 제안한다. 침입 탐지 시스템에서의 모니터링과 Data Gathering, Intrusion Detection의 기능을 분리하여 각 노드별로 역할을 달리하여 전체 노드들 중에 침입을 당한 노드에 대해서는 일정 부분을 포기하는 정도로 하여 전체적인 구조면에서 어느 정도 침입을 감내 할 수 있는 것으로 본다.

3.1 에이전트 기능

침입 탐지에 대한 개략적인 과정으로는 탐지로 의혹이 가는 모든 데이터를 수집하고,수집된 데이터에 대한 가공 및 축약, 침입을 분석 및 탐지, 침입으로 간주된 데이터에 대해서는 보고 및 조치를 취하게 된다.본 논문에서는 위의 해당 기능들을 노드별로 역할을 분담하여 애드혹 네트워크 망 전체에 대한 침입을 어느 정도 감내 할 수 있도록 한다. 다음의 그림 1은 일반 호스트 에이전트와 네트워크 모니터링을 담당하는 네트워크 에이전트의 기능의 분류를 보여준다.

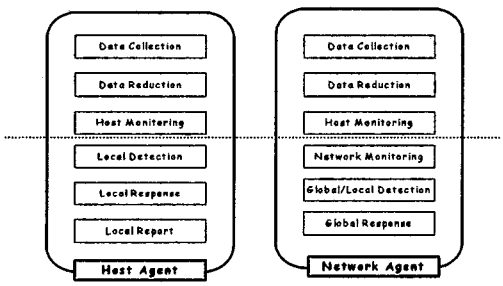

그림 1 Host Agent와 Network Agent의 기능 분류

자료 수집, 축약, 호스트 모니터링까지의 기본 기능은 호스트 에이전트와 네트워크 에이전트가 같다. 호스트 에이전트에서는 호스트 기반의 침입 탐지 시스템의 일반적인 기능들을 하고 새롭게 침입으로 탐지된 데이터를 해당 클러스터 헤드에게 보낸다. 새로운 침입 탐지 데이터를 받은 네트워크 에이전트는 애드 혹 네트워크 망 내에 있는 모든 에이전트에게 브로드 캐스팅한다. 반면에, 네트워크 에이전트는 호스트 에이전트의 역할과 더불어 클러스터내의 네트워크 공격에 대한 탐지 기능을 부여된다.

본 논문에서는 애드 혹 네트워크 상에 있는 노드들을 네트워크 패킷을 모니터링을 하는 하나의 클러스터 헤드를 가지고 있는 여러 개의 클러스터로 나누어서 관리 한다. 이는 애드 혹 이동 무선 네트워크에서의 Clusterhead Gateway Switch Routing을 응용한 것이다[2,3]

3.2 에이전트 선출 방식

네트워크 에이전트를 선출하는 방식으로는 여러 노드들 중에서 클러스터 헤드(Cluster Head)를 선출하는 CGSR 알고리즘을 응용하였다. 클러스터 헤드로 선출된 노드는 네트워크 에이전트의 기능을 부여 받게 된다. 네트워크 에이전트 선출 방식은 애드 혹 이동 무선 네트워크의 라우팅 알고리즘인 Clusterhead Gateway Switch Routing Protocol을 응용하여 만든 Clustered Network Monitoring Node Selection Algorithm을 적용하였다[2]. 선출 알고리즘을 적용하여 선출된 노드가 네트워크 모니터링을 담당하게 되는 에이전트가 된다.

Clustered Network Agent Node Selection Algorithm

첫번째, 보안에 필요한 요구사항에 맞추어 Hop수를 결정하는 단계이다. 어떤 노드에서 침입을 탐지하는 노드로의 전체 경로 Hop수가 결정되는 중요한 과정이다. 두 번째, 각 노드는 근접해 있는 노드들에게 본인이 연결되어 있는 노드들의 개수를 보낸다. 세 번째로는, 이웃 한 노드들에게서 받은 연결 개수의 합과 본인의 연결 개수를 합하여 나온 전체 연결 개수의 값을 애드 혹 네트워크 망 내의 모든 노드들에게 브로드 캐스팅 한다.네 번째, 이웃 한 노드들 중에 연결 개수가 가장 많은 노드에게 클러스터 헤드 노드를 선택하기 위한 Voting 패킷을 보낸다. 마지막으로, 적어도 하나 이상의 Voting 패킷을 받은 노드는 클러스터 헤드로 선정한다. 다음 그림 2는 네트워크 에이전트 선출 과정을 보여준다.

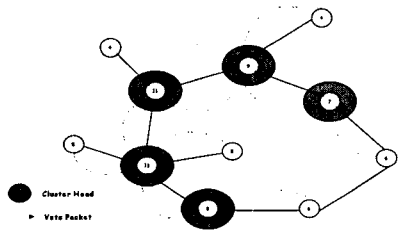

그림 2 네트워크 에이전트 선출

네트워크 에이전트로 선정이 된 노드는 Voting 패킷을 보낸 노드들과 관련된 네트워크 모니터링을 담당하게 되고, 전체적인 침입 패턴을 관리하게 된다. 호스트 에이전트에서 새롭게 추가되는 침입 패턴을 받아서 침입으로 간주가

된 데이터에 한해서 전체 네트워크 망 내의 존재하는 노드들에게 브로드 캐스팅을 하여야 한다[4].

3.3 에이전트 교체 방식

무선 애드 혹 네트워크의 특성 상 노드의 이동성이 잦으므로, 유선 네트워크 망과는 다르게 토폴로지의 변화가 많다. 다음과 같이 구성된 애드 혹 네트워크에서 노드 D가 노드 A의 범위를 벗어나게 되면 그림(a)에서 (b)로 토폴로지가 변하게 된다[5].

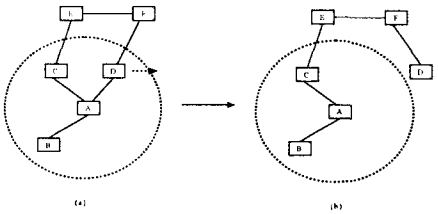

그림 3 애드 혹 네트워크에서의 토폴로지 변화

본 논문에서 제안한 네트워크 에이전트의 경우 잦은 토폴로지의 변화로 인해 접근이 불가능한 경우가 발생한다. 이런 경우를 위해서 네트워크 에이전트의 재선출 내지는 교체가 불가피하게 된다. 다음의 그림 4은 네트워크 에이전트의 교체의 경우를 보여준다.

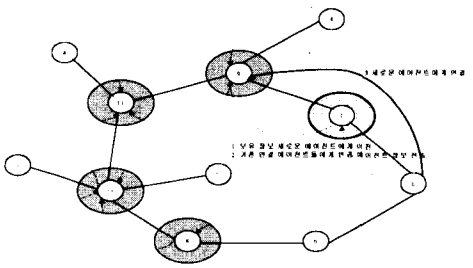

그림 4 네트워크 에이전트 교체

네트워크 에이전트가 네트워크 망을 벗어나고자 하는 경우(탈퇴 에이전트)에는 새로운 네트워크 에이전트를 재선출을 하게 된다. 탈퇴 에이전트는 연결된 에이전트들 중에 가장 근접하게 연결이 되어 있는 네트워크 에이전트에게 탈퇴 에이전트가 보유한 정보를 모두 전송하고, 탈퇴 에이전트와 연결이 되어 있는 노드들에게 네트워크 에이전트 변경 메시지를 보낸다. 변경 메시지를 받은 노드들은 새롭게 선정된 네트워크 에이전트에게 새롭게 탐지된 침입 패턴을 보고하게 된다.

일반 호스트 에이전트가 네트워크 망을 벗어나고자 하는 경우에는 네트워크 에이전트에게 탈퇴 메시지를 보내게 된다. 호스트 에이전트의 탈퇴 메시지를 받은 네트워크 에이전트는 해당 에이전트와 관련된 네트워크 모니터링을 중단하게 된다.

네트워크 에이전트가 침입을 당했을 경우에는 해당 네트워크 에이전트와 근접한 네트워크 에이전트가 모니터링하게 된다. 또한 침입을 당한 네트워크 에이전트의 경우 해당 패턴을 보유하고 있는 경우에는 다른 모든 네트워크 에이전트에게 침입에 대한 정보를 브로드 캐스팅 하여 주고, 바로 조치를 취하게 된다.

4. 결론 및 향후 연구 과제

본 논문에서는 기능별로 분리된 호스트 에이전트와 네트워크 에이전트를 이용하여 무선 애드 혹 네트워크상에서의 침입 감내 방안을 제안하였다. 네트워크를 기반으로 하는 침입 탐지 시스템의 경우 네트워크 모니터링을 담당하는 노드의 모니터링에 대한 작업량이 많다고 보고, 이러한 작업량을 분산 시킬 수 있게 하고, 이동 에이전트를 이용함으로써 침입을 감내할 수 있는 방안으로 노드들의 기능을 분산시키는 방안을 제안하였다. 본 제안은 애드 혹 네트워크 내에 적합하도록 전체 노드들을 여러 개의 클러스터 단위로 나누어서 관리를 함으로써 네트워크 모니터링의 작업량을 여러 개의 노드로 분산시킬 수가 있다. 또한 클러스터 내의 호스트 에이전트가 침입을 당했을 경우나 복구가 불가능한 경우에는 전체적인 면으로 어느 정도의 침입에 대해 감내할 수 있게 된다.

앞으로의 향후 과제로는 각 노드별 작업량을 줄일 수 있는 방안과 애드 혹 네트워크 특성에 맞는 경량의 하이브리드 침입 탐지 방안에 대한 연구가 수행되어야 할 것이다.

5. 참고 문헌

[1] Yongguang Zhang, Wenke Lee, " Intrusion Detection in Wireless Ad-Hoc Networks", Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, August 6-11, 2000.

[2] Kachirski O, Guha R, " Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks", Proceedings of the IEEE Workshop on Knowledge Media Networking, Page(s): 153 - 158, 2002.

[3] Elizabeth M.Royer, Chal-Keong Toh, " A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks", IEEE Personal Communications, April, 1999.

[4] Farooq Anjum, Amjad Umar, " Agent Based Intrusion Tolerance using Fragmentation-Redundancy-Scattering Technique", IEEE, 2000

[5] Lidong Zhou, Z. J. Haas, " Securing Ad Hoc Networks", IEEE Network Magazine, vol. 13, no.6, 1999.