제19회 한국정보처리학회 춘계학술발표대회 논문집 제10권 제1호 (2003. 5)

Mobile wireless Ad-hoc Networks 상에서의 침입탐지에 관한 연구

이재상*, 김동성*, 박종서*
*한국항공대학교 컴퓨터공학과
e-mail : {jslee, dskim, jspark}@mail.hangkong.ac.kr

A study on Intrusion Detection System for Mobile Wireless Ad-hoc Networks.

Jae Sang Lee*, Dong Seong Kim*, Jong Sou Park*
*Dept. of Computer Engineering, HanKuk Aviation University

요 약

무선기술의 발달로 인해 기존의 유선망 뿐만 아니라 무선망도 네트워크의 중요한 통신수단이 되고 있다. 그러나 이에 대한 보안 대책은 마련되지 않고 있는 실정이다. 무선 환경에서의 보안은 유선망에서의 기존의 보안 메커니즘을 사용할 수 있으나, 무선 환경의 특성을 고려할때에 동일하게 적용하기에는 어려움이 있다. 본 논문에서는 이동 무선 ad-hoc 네트워크상에서 침입에 탐지 및 대응하기 위해 IDIP와 Discovery Coorinator를 이용한 W-IDS를 제안한다.

1. Introduction

최근의 인터넷 망이 고속화되는 동시에 무선망의 사용이 크게 증가되고 있다. 그러나 이에 대한 보안 대책은 마련되지 않고 있는 실정이다. 기존 유선망의 경우처럼 보안 취약점들이 생겨났고, 이에 대한 여러 보안조치들은 효과가 없는 것이 드러났다. 또한 유선망에서 쓰이는 기술들을 무선망에 적용할 수 있는지 검증되지 못한 것들이 많다[1]. 따라서 전통적인 방화벽과 암호화 소프트웨어를 가지고 무선망을 보호하는 방법은 충분하지 않다. 따라서 이동성과 응용 프로그램을 산출하고 있는 무선 네트워크를 보호하기 위해 새로운 기술과 장치를 개발해야 한다.

Intrusion Detection system(IDS)에서도 마찬가지이다. 최근 PAN(Personal Area Network)과 같은 Ad Hoc network가 군사적인 목적뿐만 아니라, 위급상황 및 실생활에 많이 응용됨에 따라서 Ad hoc network에도 IDS가 요구되고 있다. 그러나 기존의 유선망에서 사용되는 IDS가 유선망에는 적합하지 않으므로 유선 환경에 적합하게 WIDS(Wireless Intrusion Detection System)를 설계하여야 한다. 본 논문에서는 IDIP(Intrusion Detection and Isolation Protocol)과 Discovery Coordinator를 이용한 WIDS를 제안한다.

2. 관련연구

2.1 Mobile Wireless Ad-hoc Networks

Mobile Ad-hoc Network는 기반망이 존재하지 않거나 기반망에 기초한 네트워크의 전개가 용이하지 않은 지역에서 임시적으로 네트워크를 구성하기 위해 개발된 기술로, 초기에는 군사적인 응용 목적으로 연구가 시작되었으나, 최근에는 PAN(Personal Area Network)과 같이 실생활에 적용될 수 있는 여러 분야로 응용이 확대되고 있다[2][3].

Mobile Ad-hoc Network는 이동성이 부여된 노드(Node)들이 고정된 기반망에 독립적으로 무선 인터페이스를 이용하여 자율적으로 구성하는 임시적인 네트워크이다. 이는 기반망과는 달리 중앙관리자가 존재하지 않으므로 각각의 노드들이 Host Routing을 사용하여 통신을 가능하게 한다.

Mobile Ad-hoc Network를 구성하는 노드들은 이동성을 가지기 때문에 새로운 노드의 네트워크 내부로의 진입, 네트워크 내부에서의 노드의 이동, 네트워크 외부로의 노드 이동 등은 네트워크의 토폴로지를 시간에 따라 동적으로 변화시킨다. 각 노드는 제한된 무선 전송 거리를 가지기 때문에 노드들이 서로 이동함에 따라 직접적으로 통신이 가능한 이웃 노들들의 집합 또한 함께 변하게 된다. 각 노드는 주기적으로 자신의 존재를 브로드캐스팅하며, 직접적으로 통신이 가능한 이웃 노드의 정보를 항상 유지하고, 이웃 노드의 정보에 따라 라우팅정보를 갱신한다. 이는 라우팅 프로토콜에 의해서 생성 및 관리된다.

2.2 Wireless Intrusion Detection System

Intrusion Detection System(IDS)은 네트웍이나 시스템의 침입여부를 점을 조사 및 감시하고 필요한 조치를 취하는 시스템이다[10]. IDS는 감사자료 출저에 따라 크게 호스트기반 IDS와 네트웍기반 IDS로 나뉘며, 탐지 모델에 따라 오용 탐지와 비정상 탐지로 분류된다[11].

유선환경에서 침입 탐지시스템은 다양하게 연구가 진행되고 있으며, 본 논문에서는 이를 무선 환경에 적합한 IDS를 제안하고자 한다. 기존의 IDS를 무선망에 적용시킬 때의 고려할 사항은 다음과 같다.

첫째, 무선 환경은 유선 환경에 비해 제한된 대역폭을 가진다. 무선망의 각 노드들은 각각 다른 채널들을 이용해서 통신을 하므로 각각의 IDS도 각기 다른 채널을 이용하여 통신을 한다. 이는 빈번한 통신을 해야 하는 IDS에게 통신적 제약을 주며 많은 통신 지연을 발생시킨다. 둘째, 유선환경과 마찬가지로 정상과 비정상의 구분이 쉽지 않다. 만약 어떤 특정노드에서 거짓된 정보나 갱신되지 못한 라우팅 정보를 받았을 때, 이것이 옳은 정보인지 아닌지의 구별이 어려우며, 침입자가 고의적으로 거짓된 정보를 네트웍에 흘림으로써 취약점을 유발시킨다. 셋째, 안전한 통신 채널이 필요하다. 각각의 노트의 IDS 에이전트(Agent)들 사이에는 보안 채널이 필요한데, 이는 각각의 노드가 가지고 있는 시스템, 네트웍, IDS 데이터베이스 등의 정보가 침입자에게 유출되지 않도록 하는데 꼭 필요한 것이다. 넷째, 중앙집중적 접근 및 감사 지점이 부재하다. Ad-hoc network에서는 중앙에서 제어할 수 있는 관리기의 부재는 IDS에게는 큰 문제가 된다. 이는 비정상 탐지나 오용탐지를 위한 감사자료(audit data)를 수집하는데 있어서 네트웍 트래픽이 집중되는 곳이 없기 때문이다. 다섯째, 개방 네트웍의 특성은 보안 취약성을 높이게 된다. Ad-hoc 네트웍의 특징 중 하나인 개방성은 새로운 사용자가 네트웍에 쉽게 참여할수 있는 장점이 있다. 그러나 이같은 장점은 침입자로 하여금 쉽게 네트웍에 접근할수 있다는 단점도 존재한다. 간단한 절차를 통하여 침입자가 네트웍의 정보를 획득하고 네트웍의 구성원으로써 참여할 수 있다.

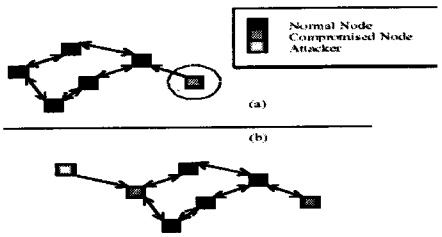

그림 1. 침해된 네트워크 노드

2.3 기존 W-IDS의 문제점

IDS는 일반적으로 높은 관리비용, 확장범위의 한계, 특별한 기능과 이를 실행시킬 수 있는 시스템을 필요로 하고, 빈번한 데이터베이스 업데이트, 수동적인 처리환경등의 문제점들을 지니고 있다. 이는 유선 환경에서도 마찬가지이다. 우선 유선의 동적인 네트웍 환경은 고정되어있는 네트웍에 비해서 안전하다고 말할 수도 있지만, 누구에게나 개방된 Air 환경을 사용하므로 안전하지 못한 측면도 있다. 이렇게 고정되어 있지 않은 네트워크의 환경은 병목지점에서 네트웍 트래픽을 모니터링하는 것을 방해한다. 따라서 중앙관리 장치가 없는 무선 Ad-Hoc Network에서는 모든 노드들이 라우팅을 해야 한다. 하지만 제한된 에너지 자원을 가진 노드로 구성되고, 한정된 대역폭을 사용해야만 하는 무선 Ad-Hoc Network에게는 큰 문제가 된다. 또한 호스트기반 모니터링도 각각의 노드들에게 많은 양의 프로세싱을 요구하므로 에너지 자원이 쉽게 고갈될 수 있다.

현재 침입자의 실제 위치를 추적하여 침입자 근처에서 해당 트래픽을 차단함으로써 침입자를 네트워크로부터 연결을 단절하고자 하는 연구가 크게 두가

지로 진행되고 있다. 첫째, DARPA의 프로젝트로써 프로토콜을 개발하거나 active network기술을 적용하는 방안에 대한 연구이다[12]. 둘째, 학계를 위주로 기존의 네트워크 기술이나 이동형 에이전트 기술을 이용하여 침입자를 탐지하거나 위치를 추적하는 방안에 대한 연구로 나누어진다[7][8].

지능형 에이전트 기반의 연구에서는 Cooperative decision algorithm을 이용한 Distributed IDS system을 제안하였다. 이 시스템에서는 각각의 Mobile Host들이 Client IDS를 탑재하고 비정상 패턴에 대한 로컬 데이터를 모니터링하고 분석하는 로컬 탐지 엔진을 작동시킨다. Cooperative detection mechanism은 IDS 프로세스에 참가하고 있는 모든 Node들이 침입 탐지가 있는지 아닌지 협동하여 결정한다. 만약 공격패턴에 대한 데이터베이스가 효과적이지 못하고 안전하지 못하다고 판단이 되면 Anomaly detection model이 사용되지만, 침입탐지에 대한 퍼포먼스가 낮고 침입탐지 경보의 오용 율이 높다.

이 접근 방식의 또 다른 문제점은 IDS의 Monolithic 디자인이다. IDS는 MAC protocols, applications, system services, network monitoring 등으로 구성되어지는데 이를 하나의 통합된 Entity로 만들어 각 노드들에게 상당한 프로세스 부담감을 준다.

Kachriski[9]의 연구에서는 기존의 Zhang[8]의 모델을 바탕으로 IDS에 Distributed multiple sensor를 사용하여 프로세스의 부하를 줄이는 방향으로 연구를 하였다. 몇몇의 노드에 센서를 탑재하여 IDS에서 모니터링 및 감지장치를 분리하였고, 이는 제한된 자원과 한정된 에너지자원을 가진 이동 노드들이 프로세스 부하를 줄이고, 효과적으로 침입을 탐지하여 탐지할 수 있도록 했다. 이는 프로세스의 부하를 줄이는 것 뿐만 아니라 네트웍을 구축하는 비용의 절감을 가능케 한다. 그러나 이렇게 이동성이 용이한 네트워크에서 각 호스트에 대한 공격을 탐지할 수 있지만 IDS 자체에 대한 공격은 탐지하기가 어렵다. IDS는 침입자를 탐지하여 탐지을 하는 것이지만 IDS 그 자체에 대한 공격에 대해서는 아직 취약점을 가지고 있다.

3. 제안 모델

3.1 제안 모델의 구조 및 구성요소

본 논문에서 제시하는 IDIP(Intrusion Detection and Isolation Protocol[11])기반의 W-IDS는 각 노드들간의 보안관련 요소 시스템들간의 협력작업을 위한 프로토콜을 포함한 보안 기반 구조이다. 구성을 보면 각각의 노드들에 W-IDS를 탑재하고, 그 중 일부의 W-IDS에는 DC(Discovery Coordinator)를 탑재한다.

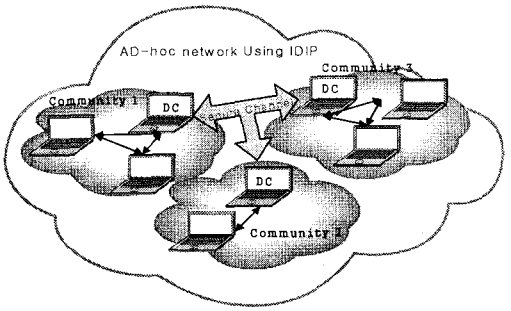

그림 2. IDIP를 사용하는 ad-hoc network

실질적으로 각 노드들은 DC를 탑재한 W-IDS를 중심으로 해서 'community'라는 하나의 작은 network를 구성하고 있으며, DC System이 'community' 내의 IDIP 기능을 제어, 관할하게 된다. 따라서 'community'는 하나의 독립된 IDIP 관리영역으로 볼 수 있다.

3.2 운용 메커니즘

이 시스템의 운용 메커니즘은 다음과 같다. 우선, 외부로부터 침입을 당하였을 경우 DC 시스템이 공격을 탐지하고, 공격이 발생하였음을 인접 'community'의 노드들과 인접한 DC 시스템에게 알리고, 공격자의 위치에 대한 역추적을 요청한다. 역추적을 요청하는 것과 동시에 동일 'community' 노드들에게 대응을 요청한다.

역추적 요청을 받은 노드는 자신이 해당 공격과 관련된 패킷을 라우팅 하였는지 혹은 호스트의 경우 해당 공격과 관련된 연결이 자신을 경유하여 나갔는지를 판단하여 그 결과를 DC에게 보고한다. 만약 자신이 공격 경로 상에 존재한다면, 피해 시스템 경로를 제외한 자신의 인접 노드에게 공격자에 대한 역추적을 계속 수행하도록 요청한다. 그리고 자신의 대응 시스템으로 공격에 대한 대응을 수행하고 그 수행 결과를 DC에게 보고한다. 이와 같은 역추적 요청에 따른 일련의 과정은, 공격자의 실제 위치가 파악될 때까지 반복하여 공격자 경로상의 노드들이 수행한다. 한편, 전체 네트워크 상에서의 대응과정은 DC가 각 노드들로부터 보고되는 정보를 가지고 협동하여 해당 공격에 대해 공격 경로를 브로드캐스팅

해서 각 노드들에게 대응을 할 수 있도록 한다.

3.3 본 제안 모델의 장점

IDIP를 이용한 W-IDS는 IDIP 자체가 보안채널을 형성하기 때문에 좀더 안정한 통신을 할 수 있고, 유선 환경의 IDIP의 기능을 대폭적으로 줄여서 사용하기 때문에 스팩이 간단하게 구성되어지며, 이를 이용하는 프로세스의 부하를 대폭 줄일 수 있다. 또한 IDIP의 보안 채널은 통신의 보안뿐만 아니라 IDS 자체의 보안 효과를 가져온다. 또한 DC의 존재는 Ad-hoc 네트웍 상에서의 manager의 기능과 auditing point를 제공해준다.

3.4 본 제안 모델의 문제점

첫째, 공격자가 목표 시스템으로 가기 위해 중간에 노드를 경유했을 경우를 위해서 DC 모든 연결에 대한 감시 기능을 수행해야 한다. 이는 DC에 상당한 프로세스 부담을 준다.

둘째, 추적 범위에 있는 community상의 모든 노드들은 자신이 라우팅 하는 모든 패킷에 대하여 로그 정보를 남기고 유지할 수 있어야 한다. 따라서 모든 노드들은 IDIP 기능이 실장 되어야 하고, DC의 경우 모든 패킷에 대해 로그를 남겨야 하는 부담을 안아야 한다.

셋째, IDIP가 실제 적용되기 위해서는 프로토콜 스택으로써 구현되어 시스템에 실장 되어야 한다. 따라서 새로운 기능을 추가하거나 기존 기능을 변경하고자 할 때, 기존에 구현된 프로토콜 스택을 변경하여야만 한다. 따라서 새로운 보안 환경변화에 유연하게 대처하거나 확장성에 있어서 한계가 있을 수 있다.

4. 결론 및 향후연구

본 논문에서는 무선 환경에서 적합한 W-IDS의 구조를 제안하였다. IDIP를 이용하여 무선 환경에서의 제약점들을 개선할 수 있는 방안을 제시하였으며, 이를 적용할 경우의 장단점에 대해서 고려해보았다. 본 논문에서 제안된 구조에 대한 기술적인 부분과 실제 적용 방법에 대한 연구가 필요하다. 또한 IDIP 기반의 W-IDS구조의 문제점 개선에 대한 연구가 필요하다.

Reference

[1] Lidong Z., Zygmunt J. H., "Securing ad hoc networks" , IEEE Network, Vol. 13, No. 6, 1999, pp. 24-30.

[2] C. K. Toh, "Ad Hoc Mobile Wireless Networks : Protocols and Systems", Prentice Hall PTR, 2002.

[3] C. E. Perkins, "Ad Hoc Networking Addison-Wesley", 2001.

[4] J. P. Macker and M. S. Corson, "Mobile Ad Hoc Networking and the IETF", *ACM Mobile Computing and Communications Review*, Vol. 2, No. 1, Jan. 1998.

[5] M. S. Corson and J. P. Macker, "Mobile Ad hoc Networking (MANET) : Routing Protocol Performance Issues and Evaluation Consi-derations", *IETF RFC 2501*, Jan. 1999.

[6] E. M. Royer and C. K. Toh, A Review of Current Routing Protocol for Ad Hoc Mobile Wireless Networks, *IEEE Personal Communications*, Apr. 1999.

[7] Wenken Lee, Yongguang Zhang, Yi-An Huang, "Intrusion Detection Techniques for Mobile wireless networks", ACM/Kluwer Wireless Networks Journal, Vol. 9, No. 5, September 2003 (To appear)

[8] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks", Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, MobiCom' 2000

[9] Oleg Kachriski and Ratan Guha, "Effective Intrusion Detection Using Multiple Sensors in Wireless AdHoc Networks", 36th Hawaii International Conference on System Sciences 2003

[10] D. Denning, "An Intrusion-Detection Model", IEEE Transactions on Software Engineering, Feb. 1987.

[11] Sandeep Kumar, Eugene H. Spafford, "A Software Architecture to support Misuse Intrusion Detection" Proceedings of the 18th National Information Security Conference 1995

[12] Schnackenberg, D. Djahandari, K. Sterne, D, "Infrastructure for intrusion detection and response", DARPA Information Survivability Conference and Exposition, 2000. DISCEX '00. Proceedings , Volume: 2 , 2000