Journal of Digital Contents Society Vol. 10 No. 3 Sept. 2009(pp. 479-484)

클러스터를 기반으로 한 침입탐지시스템

양환석*

요 약

무선 네트워크 사용이 증가하면서 무선 네트워크의 보안 시스템의 중요성이 부각되고 있는 실정이다. MANET은 이동 노드만으로 구성되어 있기 때문에 공격이 발생해도 그에 대한 탐지나 대응이 어렵다. 그리고 노드들의 이동성 때문에 유선 네트워크 환경에서 사용하던 보안 시스템을 그대로 적용하기에는 어려움이 많다. 따라서 이러한 환경에서 공격자의 악의적인 공격으로부터 시스템을 보호하고 즉각적으로 대처해야만 한다. 본 논문에서는 악의적인 공격을 탐지하고 자원의 효율적 사용을 위해서 클러스터를 헤드를 이용한 침입탐지 시스템을 제안한다. 보다 정확한 침입탐지를 위해 규칙들의 집합을 정의하고 일치 여부를 판단하는 방법을 이용하였다. 제안한 방법의 성능 평가를 위해서 blackhole, message negligence, jamming 공격을 이용하였다.

Intrusion Detection System based on Cluster

Hwan-Seok Yang

Abstract

Security system of wireless network take on importance as use of wireless network increases. Detection and opposition about that is difficult even if attack happens because MANET is composed of only moving node. And it is difficult that existing security system is applied as it is because of migratory nodes. Therefore, system is protected from malicious attack of intruder in this environment and it has to correspond to attack immediately. In this paper, we propose intrusion detection system using cluster head in order to detect malicious attack and use resources efficiently. we used method that gathering of rules is defined and it judges whether it corresponds or not to detect intrusion more exactly. In order to evaluate performance of proposed method, we used blackhole, message negligence, jamming attack.

Keywords : Intrusion Detection System, System Security, Mobile Ad hoc Network

1. 서 론

네트워크 기술이 빠르게 발전하고 인터넷이 광범위하게 보급되면서 다양한 부작용이 발생하고 있다. 컴퓨터 바이러스에 의한 자료의 파괴 및 유출, 해킹에 의한 개인 정보의 유출 그리고 웜이나 DoS 공격에 의한 네트웍 자원의 고갈 등 다양한 부작용이 있다. 따라서 이러한 부작용에 대한 대처가 필요한 상황이다. 또한 네트워크의 공격들로 인한 피해는 점차적으로 증가하고 있는 추세이다. 대부분의 공격들은 현재 대부분 패치가 되어있지만, 어떤 변형된 웜이나 바이러스가 발생할지 모르는 일이다. 따라서 개인의 정보보호 및 네트워크의 보호와 침입에 대한 즉각적인 조치가 필요하다. 현재까지 대중화 되어있는 보안 시스템들은 침입차단 시스템(방화벽), 침입탐지 시스템(Intrusion Detection System : IDS), 침입방지 시스템(Intrusion Prevention System : IPS) 들이 있다[1]. 방화벽은 접근 제어 리스트를 통해서 접근의 허용 여부를 결정하는 방식이다. 이 방식의 단점은 접근제어가 허용되는 경로를 통하여 공격이 이루어지는 경우에는 이를 막을 수 없게 된다. 침입탐지 시스템은 트래픽 감시를 통해서 공격을 탐지하는 시스템이다. 만약 트래픽에 이상이 감지되면 관리자에게 경고 메시지를 전달하여 적절한 조치

※ 제일저자(First Author) : 양환석
접수일:2009년 7월 30일, 완료일:2009년 9월 29일
* 호원대학교 사어버수사경찰학부 연구교수
badhack@howon.ac.kr

를 취하도록 한다. 침입방지 시스템은 방화벽과 침입탐지 시스템이 가지는 장점을 모두 가지고 있으며 최근 보안 분야에서 널리 사용되고 있다.

그리고 최근에는 네트워크 시장의 빠른 변화와 무선 인터넷의 사용이 증가하면서 무선 랜을 이용한 네트워크의 연결은 점차 증가하였으며, 이는 네트워크의 침입과 공격이 유선 환경에서 무선 환경으로 확대되어 발전하는 계기가 되었다. 무선 링크를 사용하는 무선 네트워크는 유선 네트워크에 비해 보안상 취약한 부분이 많다. 특히 단말기들의 이동성 문제로 인하여 보안에서 심각한 문제를 가지고 있다. 이러한 무선 네트워크의 취약점으로 인한 공격으로는 스니핑(Sniffing) 툴을 사용한 공격, 스푸핑(Spoofing)을 이용한 공격, 플러딩(Flooding) 공격, 서비스 거부(Denial of Service) 공격과 분산 서비스 거부(Distributed-Denial of Service) 공격의 형태로 분류할 수 있다[2]. 따라서 무선 환경에서 안전한 통신을 보장하기 위해서는 무결성(Integrity), 가용성(Availability), 신뢰성(Confidentiality), 인증(Authentication) 그리고 부인봉쇄(Non-Reputation)와 같은 보안 서비스를 제공해야 한다[3]. 따라서 무선을 이용한 침입이 유선에 비해 더욱 다양하고 쉽기 때문에 더욱 보안에 신경을 써야만 한다.

본 논문에서는 네트워크를 구성하는 노드들을 클러스터로 형성한 후 노드의 연결수와 신뢰도 값을 이용하여 클러스터 헤드를 선출한다. 그리고 선출된 클러스터 헤드가 클러스터 내의 침입탐지를 수행하는 침입탐지 시스템을 제안하였다. 그리고 보다 정확한 침입탐지를 위해서 규칙들의 집합을 정의하고 이와 일치 여부를 판단하여 침입을 탐지하도록 하였다. 기존의 침입탐지시스템은 오탐지 비율이 높거나 알려지지 않은 침입에 취약한 단점을 가지고 있다. 본 논문에서 제안한 침입탐지 방법은 자신의 이웃 노드로 전송된 메시지를 분석하는 동안에 클러스터 헤드에 의해서 검출된 네트워크 실패 횟수를 계산하여 침입탐지를 수행하게 된다.

본 논문의 구성은 다음과 같다. 2장에서는 침입탐지시스템의 탐지 기법과 침입방지 시스템에 대하여 살펴보고 3장에서는 본 논문에서 제안한 방법에 대하여 설명하였다. 4장에서는 제안한 방법의 성능을 평가하고 마지막으로 5장에서는 결론을 맺는다.

2. 관련연구

침입탐지 시스템은 탐지 기법에 따라 비정상행위 탐지(Anomaly Detection)와 오용 탐지(Misuse Detection)로 분류할 수 있다. 비정상 행위 탐지는 침입에 대해 미리 만들어 둔 데이터와 비교 분석하여 침입을 탐지하는 방법이다. 먼저 정상적인 시스템의 프로파일을 유지하고 이 프로파일에 어긋나는 행위를 탐지하게 된다. 비정상 행위 탐지는 알려지지 않은 새로운 공격에 대해서도 탐지가 가능한 장점이 있지만 정상적인 행위에 대한 데이터를 유지해야하고 비정상 행위를 판단하기 위한 데이터 분석에 많은 비용이 드는 단점을 가지고 있다. 비정상 행위 탐지를 위한 접근 방식으로는 과거의 통계자료를 바탕으로 현재 프로세스의 행위를 관찰하여 프로파일 작성하고 이를 이용하여 침입을 탐지하는 통계적인 접근 방법과 특정 순간까지 발생한 이벤트들을 기반으로 다음 이벤트를 예측하는 방법으로 예측된 이벤트가 아닌 다른 이벤트가 발생할 경우 이를 침입으로 간주하는 탐지 방법이다. 오용 탐지는 시스템의 잘 알려진 취약점에 대해 잘 정의된 패턴 정보를 가지고 실제적인 공격이 시도될 때 이를 탐지하는 방식으로서 비정상 해위 탐지 방법에 비해 구현이 쉽고 정확성 또한 높기 때문에 현재 가장 많이 사용하고 있는 탐지 기법이다[4]. 그러나 최신의 공격에 대해서는 규칙을 추가해야 한다는 단점이 있다.

네트워크 구성 방법에 따라 네트워크 기반 IDS와 호스트 기반 IDS로 나눌 수 있다[5]6]. 네트워크 기반 IDS는 네트워크 내에 모든 패킷을 수신하고 분석하여 침입 여부를 판단한다. 네트워크 기반 IDS는 네트워크 마다 하나만을 설치하기 때문에 번거롭지 않다. 반면에 성능에 대한 요구 사항 때문에 서명 분석(signature analysis)을 하는 경우가 많은데, 잘 알려진 공격을 탐지하는 능력을 뛰어나지만 알려지지 않은 공격이나 변형된 공격에는 탐지가 어렵고 암호화된 세션에 대한 침입탐지에도 취약하다[7].

호스트 기반 IDS는 감사(audit)기록이나 파일

시스템 감시를 통해 침입을 탐지한다. 호스트 기반 IDS는 non-promiscuous 모드에서 동작하고 이는 더 많은 시스템에서 사용될 수 있다는 장점이 있다. 호스트 기반 IDS의 또 다른 장점은 필요에 맞게 규칙을 조정할 수 있다는 것이다. 이렇게 해당 규칙들의 조합을 적용하여 사용하는 것은 전체 규칙들을 적용하는 것보다는 시스템의 부하를 줄일 수 있고, 이는 시스템의 성능 향상을 유도할 수 있다. 하지만 호스트 기반 IDS는 보호하고자 하는 모든 시스템에 설치해야 한다는 단점이 있다.

침입탐지 시스템은 침입이 발생해야만 그에 따른 탐지나 대책이 발생하는 사후조치에 해당되고, 오탐지율이 높게 발생할 경우 시스템의 성능 저하를 유발시킨다. 따라서 대부분의 사용자들이 사고가 일어나기 전에 미리 사고를 예측하고 방지하여 자신들의 정보를 보호받고자 하는 변형체가 침입방지 시스템(Intrusion Prevention System)이다.

침입방지 시스템은 탐지된 공격이 실제 피해를 주기 전에 미리 능동적으로 차단함으로써 피해를 최소화할 수 있는 보안 솔루션이다. 운영체제나 응용 프로그램의 취약점을 미리 보완하고 웜이나 버퍼 오버플로우, 비정상적인 트래픽이나 알려지지 않은 공격까지 차단할 수 있는 보안 능력을 제공해준다. <표 1>는 침입방지 시스템의 장단점으로 보여주고 있다.

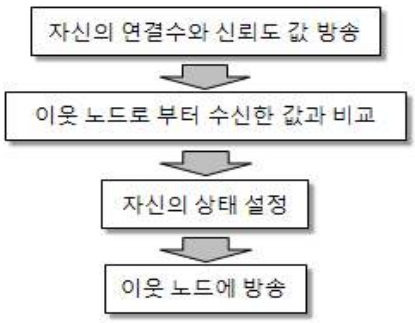
<표 1> 침입방지 시스템 특징

	침입방지 시스템
장 점	· 웜의 전파 차단 · 새로운 공격에 대처 가능 · 응용에 대해 특정 보호 가능 · 시스템 관리자의 부담 감소
단 점	· 보안 도구가 되기 위해 튜닝 필요 · 보안 업데이트에 의존도가 높음 · 서버에 도달하는 지연 시간이 길어짐

3. 제안한 방법

3.1 클러스터 형성 및 관리

본 논문에서는 MANET을 구성하는 노드들 사이의 안전한 통신을 제공하고 비정상 노드를 효율적으로 탐지하기 위해 클러스터를 이용하였다. 클러스터를 형성하는 과정은 클러스터 헤드 선출과 게이트웨이 노드, 멤버 노드로 이루어진다. 먼저 클러스터 헤드는 이웃 노드들과의 연결수와 신뢰도 값이 가장 높은 노드가 된다. 여기서 연결수를 이용하는 이유는 많은 노드들의 정보를 유지할 수 있기 때문이다. 그리고 신뢰도 값이란 이웃 노드가 자신의 패킷을 성공적으로 전달해 준 값을 의미한다. 이 신뢰도 값을 이용함으로써 노드들의 이기적 행동을 방지함으로써 노드들의 신뢰성을 높일 수가 있기 때문이다. 클러스터 헤드의 역할은 멤버 노드들과 클러스터를 관리하는 기능뿐만 아니라 IDS의 역할을 수행하게 된다. 이렇게 선출된 클러스터 헤드가 다른 클러스터의 멤버 노드라면 두 번째로 높은 값을 갖는 노드를 클러스터 헤드로 선택한다. (그림 1)은 클러스터를 형성하는 과정을 보여주고 있다.



(그림 1) 클러스터 형성 과정

3.2 침입탐지 알고리즘

본 논문에서 제안한 침입탐지 알고리즘은 다음과 같은 세단계로 이루어져 있다.

(1) 1단계 : promiscuous 모드에서 데이터수집

(2) 2단계 : 수집한 데이터에 규칙을 적용

(3) 3단계 : 침입탐지

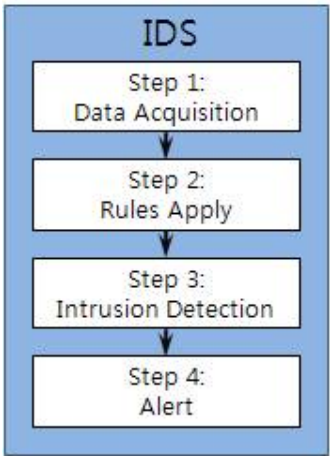
각 단계별 기능을 살펴보면 다음과 같다. 먼저 첫 번째 단계는 침입탐지를 위한 데이터 수집 단계이다. 이 단계에서 감시 노드는 promiscuous 모드로 메시지를 감시하다가 의심스러운 정보가 발견되면 이 메시지를 저장한다. 메시지로부터 추출된 데이터는 배열에 저장된다. 배열에 저장된 데이터의 삭제는 지정된 시간이 초과하거나 메모

리의 양이 부족할 때는 이루어진다. 두 번째 단계는 수집된 데이터에 규칙을 적용하는 단계이다. 배열에 저장된 데이터들이 이미 정의되어 있는 규칙에 해당되는지를 평가하게 된다. 만약 어느 규칙에도 해당되지 않는다면 실패 카운터 값을 증가시키고 메시지를 삭제한다. 무선 노드들은 제한된 자원을 이용해야 하기 때문에 불필요한 데이터를 삭제하는 것이 유리하다. 이렇게 함으로써 실행 시간, 탐지 시간을 줄일 수 있다.

다음은 두 번째 단계에서 침입탐지를 위해 사용한 규칙에 대한 정의이다. 첫 번째로 Interval 규칙은 제한된 크기보다 크거나 작은 두 개의 연속적이 메시지를 수신하는 사이에 시간이 지난 경우 실패가 발생한다. 이웃 노드에 의해 생성된 데이터 메시지를 송신하지 않는 negligence 공격 그리고 자기 이웃의 에너지 소모량을 증가시키기 위해 메시지 송신 비율을 증가시키는 소모 공격은 이 규칙에 의해 검출될 수 있다. 두 번째로 retransmission 규칙은 수신한 메시지를 자신의 이웃 노드에게 전달하는지를 감시한다. 이 규칙에 의해 검출될 수 있는 두 가지 공격은 blackhole과 선택적 포워딩 공격이다. 세 번째로 repetition 규칙은 똑같은 메시지는 같은 이웃에 의해 제한된 횟수만큼 재전송될 수 있다. 이 규칙은 침입자가 어디서 똑같은 메시지를 몇 번 송신했는지를 검출할 수 있다. 그러므로 DoS 공격에 대응할 수 있다. 네 번째로 Delay 규칙은 모니터의 이웃 노드에 의해 재전송되는 메시지는 정의된 시간 안에 이루어져야 한다. 그렇지 않으면 공격으로 검출된다. 다섯 번째로 Integrity 규칙은 수신된 메시지의 내용을 수정하는 공격은 이 규칙에 의해 검출된다. 마지막으로 Jamming 규칙은 모니터에 의해 보내진 메시지의 충돌 횟수는 네트워크 내에서 기대 수보다는 적어야만 한다. 네트워크 안에 잡음을 만들고 통신 채널을 왜곡시킬 수 있는 jamming 공격은 이 룰에 의해 검출된 수 있다.

마지막으로 침입탐지 단계이다. 이 단계에서는 공격자의 의도에 의해 마치 네트워크 문제인 것처럼 보이는 공격을 탐지해 낼 수 있는 능력을 향상시키기 위해 클러스터 헤드 노드에 감시 기능을 추가하는 방법을 제안하였다. 그리고 네트워크 상에 의심스러운 노드의 행동 목적을 추론할 수 있도록 하였다. 이렇게 함으로써 data alteration, message negligence, blackhole, selective forwarding, jamming과 같은 공격에 의해 생긴 문제들을 보다 쉽게 해결할 수 있게 되었다.

본 논문에서 제안한 침입탐지 방법은 자신의 이웃 노드로 전송된 메시지를 분석하는 동안에 감시 노드에 의해서 검출된 네트워크 실패 횟수를 카운트한 후 이 수가 만약 기대 수치보다 크다면 공격이 발생한 것으로 판단한다. 이 수는 자신의 이웃 노드에 있는 각 노드에 대한 실패 기록을 이용하여 감시 노드에 의해 동적으로 계산된다. 그리고 각 이웃 노드에 대한 실패의 평균값은 감시 노드에 의해 유지 및 갱신된다. (그림 2)는 감시 노드의 침입탐지 단계를 보여주고 있다.



(그림 2) 침입탐지 과정

4. 실험 및 결과

4.1 실험환경

본 논문에서 제안한 클러스터 기반 침입탐지 시스템의 성능 분석을 위하여 다음과 같은 실험 환경을 이용하였다.

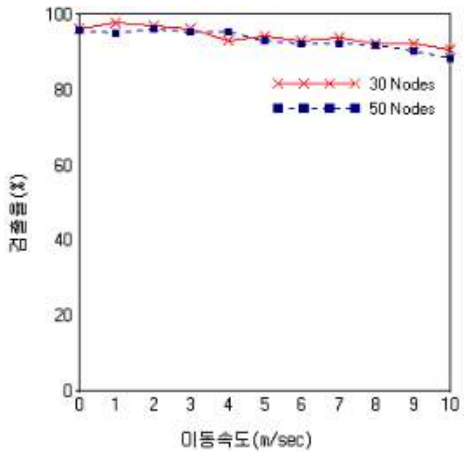
<표 2> 실험에 사용한 환경 변수 값

환 경 변 수	값
이동성 모델	Random waypoint model
무선 전송 모델	Two-Ground(1/r4)
MAC 프로토콜	IEEE 802.11 DCF
대역폭	2Mbps

본 논문에서 노드들의 이동 속도는 0m/s ~ 10 m/s, 노드들의 정지 시간은 30초, 패킷의 크기는 64 bytes, 데이터 전송 범위는 200m로 하였다. 실험에 사용한 노드의 수는 30개와 50개이고 노드 수에 따른 네트워크의 크기는 각각 달리하였으며 각 실험 시간은 300초로 하였다. 본 논문에서 실험에 사용한 노드는 제한된 방향성을 가진 공간보다는 사용자가 자유롭게 움직일 수 있는 개방된 환경 하에서 동작한다고 가정한 것이다.

4.2 실험 환경

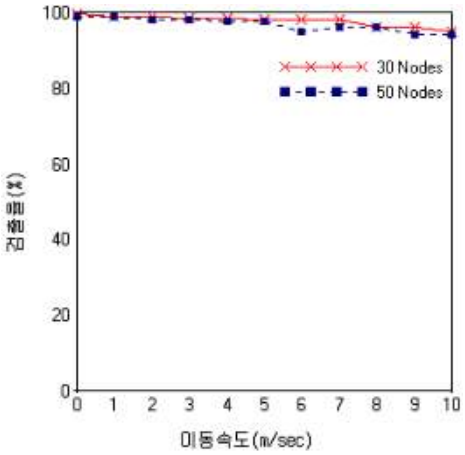
침입탐지 실험을 위해 message negligence, jamming, repetition 공격을 이용하였다. 각 공격은 임의로 발생시켰으며 실험 시간 동안 50번 발생시켰다. 실험에서 감시 노드는 수집된 데이터를 정의된 규칙에 적용하여 침입탐지 및 공격의 유형을 알아내게 된다.



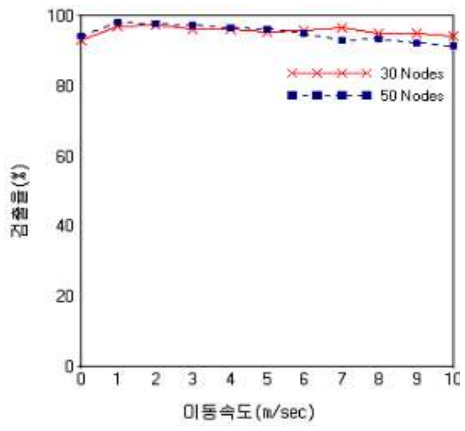
(그림 3) Message negligence attack 탐지

(그림 3)에서는 이웃 노드에서 생성된 메시지를 송신하지 않는 message negligence 공격의 탐지율을 보여주고 있다. 이 공격은 클러스터 헤드가 이웃 노드의 행동을 감시하고 있기 때문에 높은 탐지율을 보여주고 있다. 특히 노드들은 이웃 노드로부터 수신한 메시지를 전송하지 못하게 되면 자신의 신뢰도 값이 떨어지게 된다. 그림에서 나타나듯이 노드들의 이동 속도가 빨라짐에 따라 공격의 오탐지율이 약간 높아졌다. 왜냐하면 노드들의 이동 속도에 따라 목적지 노드까지의 경로를 찾는데 실패를 하는 경우가 발생하였기 때문이다.

(그림 4)는 Jamming 공격 탐지율을 보여주고 있다. 네트워크 내에 잡음을 만들고 통신 채널을 왜곡시킬 수 있는 jamming 공격도 쉽게 탐지해 낼 수 있었다. Jamming 공격은 클러스터 헤드나 게이트웨이 노드에 의해 보내진 메시지의 충돌 횟수는 네트워크내의 기대 수보다 적어야 한다. 만약 기대 수치보다 크게 된다면 이를 공격으로 간주하게 된다. 그림 4에서 나타나듯이 노드의 수가 많고 이동 속도가 빠를수록 패킷의 충돌 횟수가 증가함에 따라 자연스러운 네트워크 오류를 공격으로 잘못 탐지하는 비율이 약간은 높아졌다.



(그림 4) Jamming attack 탐지



(그림 5) Repetition attack 탐지

(그림 5)에서는 Repetition 공격 탐지율을 보여주고 있다. 공격자에 의해 똑같은 메시지를 무차별적으로 송신하는 이 공격도 다른 공격들과 마찬가지로 쉽게 탐지해 낼 수 있었다. 왜냐하면 각 노드에서 전송되는 데이터는 클러스터 헤드를 거쳐야 하기 때문에 공격자가 어디서 똑같은 메시지를 몇 번 송신했는지를 알 수 있게 되는 것이다.

5. 결론

본 논문에서는 연결수와 신뢰도 값을 이용해 클러스터 헤드를 선출한 후 새롭게 정의한 규칙을 기반으로 한 침입탐지 시스템을 제안하였다. MANET에서는 이동 노드들로만 구성되어 있기 때문에 공격이 발생해도 그에 대한 탐지나 대응이 어렵다. 따라서 이러한 문제를 해결하게 위해 MANET을 클러스터로 형성하고 클러스터 헤드를 이용하여 침입탐지를 수행하였다. 클러스터 헤드를 선출할 때 연결수와 신뢰도 값을 이용하였다. 이 두 가지를 이용함으로써 노드들의 이기적 행동을 방지하고 신뢰성을 높일 수가 있기 때문이다. 그리고 공격자의 악의적인 공격을 탐지하고, 오탐지율을 낮추기 위해서 다양한 공격에 대한 규칙을 정의하였다. 이렇게 함으로써 네트워크 내의 공격과 비정상 행동을 하는 노드를 쉽게 파악할 수 있게 되었으며 공격의 오탐지율을 낮추게 되었다. 향후 연구로는 이동 노드들의 자원 문제와 데이터 전송 효율성에 대한 연구가 이루어져야 할 것이다.

참 고 문 헌

[1] Guorui Li, "A Distributed Intrusion Detection Scheme for Wireless Sensor Networks", the 28th International Conference on Distributed Computing Systems Workshops, June 2008.

[2] Peng Ning, "Mitigating DoS Attacks against Signature-Based Broadcast Authentication in Wireless Sensor Networks", ACM journal no.20, 2005.

[3] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks:Attacks and countermewsures", in the Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.

[4] J. Deng, R. Han, and S. Mishra, "A performance evaluation of intrusion-tolerant routing in wireless sensor networks", In Proceeding of IEEE 2nd Int'l Workshop on info Processing in Sensor Networks, April 2003.

[5] Salvatore J. Stolfo, et al., "Anomaly Detection in Computer Security and an Application to File System Accesses", Proceedings of 15th International Symposium of Foundations of Intelligent Systems, 2005.

[6] Shi Zhong, Taghi M. Khoshgoftaar, and Naeem Seluya, " Evaluating Clustering Techniques for Network Intrusion Detection.", In Proceeding of the 10th ISSAT International Conference on Reliability and Quality and Design, pp.149-155. Las Vegas, Nevada, 2004.

[7] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense aginst wormhole attacks in wireless networks", In Proceeding of IEEE Infocomm, pp.349-364, 2003.

양 환 석

1998년 : 조선대학교 전산통계학과 대학원 (이학석사)

2005년 : 조선대학교 전산통계학과 (이학박사)

2007년~현 재: 호원대학교 사이버수사경찰학부 연구교수

관심분야 : 시스템 보안(System Security), 정보보안(Information Security)