클러스터링 기법을 이용한 침입 탐지 시스템의 경보 데이터 상관관계 분석

신 문 선[†] · 문 호 성[††] · 류 근 호[†††] · 장 종 수[††††]

요 약

이 논문에서는 침입 탐지 시스템의 탐지 효율을 높이기 위해 데이터 마이닝의 클러스터링 기법을 이용하여 경보 데이터를 그룹화하고 그 결과를 이용하여 경보 데이터의 상관 관계를 분석하는 방법을 제안하였다. 즉, 클러스터링 기법을 이용하여 경보데이터를 사용자가 원하는 개수의 그룹으로 분류하고, 생성된 경보 데이터 클러스터 모델을 이용하여 새로운 경보 데이터를 분류할 수 있도록 하였다. 또한, 결과 클러스터의 생성 원인이 되는 이전의 경보의 분포 데이터를 저장 관리하여 클러스터 간의 시퀀스를 생성하였고, 생성된 각각의 클러스터 시퀀스를 통합하여 클러스터들의 시퀀스를 추출하여 발생한 경보 이후의 향후 발생 가능한 경보 타입을 예측하기 위한 방법을 제공하였다. 이는 과거에 탐지된 공격의 형태뿐만 아니라 새로운 혹은 변형된 경보의 분류나 분석에도 이용 가능하다. 또한 생성된 클러스터간의 생성 원인의 분석에 의한 클러스터 간의 순차적인 관계의 추출을 통해 사용자가 공격의 순차적 구조나 탐지된 각 공격 이면에 감추어진 전략을 이해하는데 도움을 주며, 현재의 경보 이후에 발생 가능한 경보들을 예측할 수 있다.

Alert Correlation Analysis based on Clustering Technique for IDS

Moon Sun Shin[†] · Ho Sung Moon[††] · Keun Ho Ryu[†††] · Jong Su Jang[††††]

ABSTRACT

In this paper, we propose an approach to correlate alerts using a clustering analysis of data mining techniques in order to support intrusion detection system. Intrusion detection techniques have been developed to protect computer and network systems against malicious attacks. However, intrusion detection techniques are still far from perfect. Current intrusion detection systems cannot fully detect novel attacks or variations of known attacks without generating a large amount of false alerts. In addition, all the current intrusion detection systems focus on low-level attacks or anomalies. Consequently, the intrusion detection systems usually generate a large amount of alerts. In situations where there are intensive intrusive actions, it is difficult for users or intrusion response systems to understand the intrusion behind the alerts and take appropriate actions. The clustering analysis groups data objects into clusters such that objects belonging to the same cluster are similar, while those belonging to different ones are dissimilar. As using clustering technique, we can analyze alert data efficiently and extract high-level knowledge about attacks. Namely, it is possible to classify new type of alerts as well as existed. And it helps to understand logical steps and strategies behind series of attacks using sequences of clusters, and can potentially be applied to predict attacks in progress.

키워드 : 침입 탐지(Intrusion Detection), 경보 데이터(Alert Data), 경보 상관관계(Alert Correlation), 클러스터링(Clustering)

1. 서 론

다양해지고 새로워지는 침입을 효율적으로 탐지하고 방어하기 위해서 침입 탐지 시스템은 보다 많은 양의 룰을 구축하여야 하며 이러한 룰을 찾아내기 위한 구조적인 메커니즘이 필요하다. 또한 과거의 침입 데이터로부터 새로운 형태의 침입을 유추할 수 있는 방법론도 필요하다. 그러나, 현재의 침입 탐지 시스템은 단순히 네트워크 상의 혹은 호스트로 유입되는 개개 패킷 수준에 대한 탐지에 초점이 맞춰져 있기 때문에, 각각의 공격이 의도하는 전략이나 각 공격 이면의 논리적인 단계와 같은 고수준의 의미를 포착하기가 용이하지 않다. 또한 침입 탐지 시스템이 생성하는 대량의 로그 파일은 분석하는 것뿐만 아니라 적절하게 다루는 것조차도 불가능하다.

따라서, 이러한 문제점을 해결하기 위해서 이 논문에서는 데이터 마이닝 기법을 이용하여 경보 데이터를 분석하여 그들간의 순차적인 상관관계를 추출하는 방법을 제안한다. 침입 탐지 시스템의 탐지 효율을 높이기 위해 데이터 마이닝

※ 이 연구는 한국전자통신연구원과 한국과학재단 RRC(청주대 ICRC) 및 대학 IT 연구센터 육성 지원사업의 연구비지원으로 수행되었음.
† 정 회 원 : 충북대학교 대학원 전자계산학과
†† 준 회 원 : 가림정보기술
††† 종신회원 : 충북대학교 전기전자및컴퓨터공학부 교수
†††† 정 회 원 : 한국전자통신연구원 책임연구원
논문접수 : 2003년 6월 24일, 심사완료 : 2003년 8월 13일

의 클러스터링 기법을 이용하여 경보 데이터를 그룹화한다. 그리고 생성된 클러스터 모델을 이용하여 새로운 경보가 들어오면 적당한 클러스터로 분류한다. 또한, 결과 클러스터의 생성 원인이 되는 이전의 경보의 분포 데이터를 저장 관리하여 클러스터간의 시퀀스를 생성하고, 생성된 각각의 클러스터 시퀀스를 통합하여 클러스터들간의 시퀀스를 추출한다. 추출된 시퀀스는 발생한 경보 이후의 향후 발생 가능한 경보 타입을 예측하기 위한 방법을 제공한다.

이 논문에서 제안한 클러스터링을 이용한 경보 데이터의 분석 방법은 먼저, 데이터간의 유사성을 이용한 경보 데이터의 그룹화를 통해 생성된 모델을 이용하여 새로운 경보 데이터에 대한 분류를 자동화하고, 또한 생성된 클러스터간의 생성 원인의 분석에 의한 클러스터간의 순차적인 관계의 추출을 통해 공격의 순차적인 구조를 예측하고, 현재의 경보 이후에 발생 가능한 경보들을 예측 가능하게 한다.

논문의 나머지 부분은 다음과 같이 구성하였다. 2장에서는 관련 연구로써 경보 데이터의 상관관계 분석과 클러스터링 기법에 대해 설명하고 3장에서는 경보 데이터에 클러스터링 기법을 적용하여 분류 모델과 예측 모델을 생성하기 위한 절차에 대해 기술한다. 4장에서는 구현을 위한 시스템의 구성에 대해 기술하고 5장에서는 구현된 시스템의 실험적인 평가와 결과에 대해 기술한다. 마지막으로 6장에서 결론을 맺는다.

2. 관련 연구

최근 침입 탐지 시스템의 성능향상과 알려지지 않은 공격에 대응하기 위한 방안으로 경보 상관관계 분석에 대한 연구가 진행되고 있다. 이는 보안 서비스의 질을 향상시키며 능동적인 보안이라는 측면에서 중요한 의미를 가진다. 이 장에서는 경보데이터의 상관관계 분석에 대한 기존의 연구들을 살펴 본다.

경보 상관관계 분석은 경보 데이터간의 연관성 분석을 통해, 새로운 공격의 탐지나 보다 정확한 탐지를 위한 침입 탐지 모델을 구축하고, 사용자에게는 보다 이해하기 용이한 정보를 제공하는 것이 그 목적이다. 개연적 경보 상관관계 분석은 경보 데이터의 속성의 유사성을 이용하여 경보 데이터 간의 상관관계를 분석하는 기법이다[1]. 속성간의 유사성을 이용하여 공격 타입 간의 유사성을 정의하고 이를 이용하여 공격 타입 간의 연관 관계를 추출한다. 그러나 이 방법은 선택된 속성에 의존적이며, 경보 데이터간의 인과관계를 완벽하게 탐사하기에 적당하지 못하다는 단점을 가지고 있다. [2]에서는 발견 학습을 이용한 접근 방법을 "취약성 침입(stealthy portscan)"을 탐지하기 위해 적용하였다. 취약성침입은 비정상적인 패킷을 던져주고 그 반응에 따라 포트스캔(port scan)하는 것을 말한다. [2]에서 비록 발견 학습을 경보 데이터 상관관계 분석에 이용하였지만, 이 방법 또한 경보 데이터간의 인과 관계를 완벽하게 분석하지 못하였다. [3]은 경보 데이터의 통합과 상관관계 분석 기법을 제안하였다. 특히, [3]에서 제안된 상관관계 분석 방법은 어떤 타입의 경보가 주어진 경보 유형의 다음에 오는지를 기술하기 위한 결과 메커니즘을 이용하였다. 이것은 오용 탐지 기법과 유사하다. 그러나 이 결과 메커니즘은 단지 경보의 유형과 경보에 의한 취약점 탐사 공격인 프로브(probe), 보안 레벨, 결과 정의에 포함된 두 경보간의 시간 간격만을 사용하며, 가능한 모든 경보 데이터들이 서로 관련되기 위한 충분한 정보를 제공하지 않는다는 단점이 있다. 게다가 공격자가 어떻게 공격의 시퀀스를 조정할 것인지 예측하는 것 또한 쉽지 않다. 또 다른 접근 방법으로 공격 시나리오가 포함되어 있는 학습 데이터 집합에 기계 학습 기법을 적용하여 경보 상관관계 모델을 학습하는 기법이 있다[4]. 이 방법은 경보 데이터의 상관관계 분석을 위한 모델을 자동적으로 생성할 수 있는 장점이 있지만, 매 적용마다 학습이 필요하며, 결과 모델이 학습 데이터에 의존적이므로 학습 데이터에 포함되지 않은 공격 시나리오는 탐지할 수 없는 단점이 있다.

프랑스의 CERT에서는 경보 데이터 관리를 위한 데이터베이스 스키마를 설계하고 XML형태의 경보들을 통합하여 클러스터링과 병합과정을 거쳐 상관관계분석을 하고 공격에 대한 global 진단을 결정하는 프레임워크를 마련하는 프로젝트[5]를 진행 중에 있다. 이 경우 다양한 침입 탐지 시스템으로부터의 경보를 통합하고 관리하기 위한 기능을 제공하고 있다.

클러스터링은 잠재적인 데이터에서 그룹들을 탐사하거나 관심있는 분포를 확인하는데 유용한 방법이다[6]. 이 기법은 개체들의 집합을 개체의 클래스들로 그룹화하는 절차이다. 이때, 동일한 클러스터에 속하는 개체들은 유사성을 가지고, 다른 클러스터에 속하는 개체들은 상서성을 가진다. 대량의 데이터로부터 클러스터링을 수행하기 위한 기법에는 여러 가지 방법이 있지만, 크게 부분적인 클러스터링 기법과 계층적인 클러스터링 기법으로 분류된다[6]. 부분적인 클러스터링 기법은 주어진 n개의 개체 집합에 대해 k개의 파티션을 생성하고, 어떤 클러스터에 포함된 개개의 개체와 해당 클러스터 중심과의 유사도 측정을 통해 데이터를 클러스터에 재배치한다. 이렇게 초기에 생성된 클러스터를 정련하는 과정을 통해 최종 클러스터를 형성한다. 이 기법은 속도 면에서는 우수한 편이지만, 초기 클러스터의 선택에 따라 클러스터의 결과가 달라지며, 아웃라이어(outlier)의 처리에 미숙하다는 단점이 있다. 아웃라이어란 특정 클러스터에 포함되

지않는 유사성이 먼 개체들을 의미하며 이들을 가까운 클러스터에 포함시킬 것인지에 관한 문제가 아웃라이어 처리문제이다. 계층적인 클러스터링 기법은 개체들의 계층적인 분해를 통해 클러스터링을 수행하는 기법이다. 이 기법은 상향식 혹은 하향식으로 수행될 수 있는데, 하향식 알고리즘은 먼저 개체 개개를 각각 하나의 클러스터로 인식하고, 이를 유사성 측정 기준에 의해 유사한 그룹으로 통합하는 방식이다. 이 클러스터링 과정은 모든 개체가 하나의 그룹으로 통합되거나 사용자가 원하는 어떤 시점에서 종료된다. 상향식 클러스터링 알고리즘은 하향식의 반대 전략을 따른다. 상향식 알고리즘은 주어진 모든 개체를 하나의 그룹으로 인식하여, 각각의 개체가 각각 하나의 클러스터를 이루거나, 사용자가 원하는 클러스터의 수를 가질 때까지 그룹을 분해하는 방법이다. 이 논문에서는 클러스터링 기법 중 상향식의 계층적인 클러스터링 기법인 CURE 알고리즘을 기반으로 경보데이터의 유사성에 따른 클러스터의 생성과 생성된 클러스터간의 시퀀스 유추를 통한 경보 상관관계 분석을 시도한다.

3. 경보 데이터의 상관관계 분석 절차

이 장에서는 경보 데이터를 데이터베이스에 저장하기 위한 스키마를 설계한다. 또한 경보 데이터에 클러스터링 분석을 적용하기 위하여 경보 데이터간의 유사성을 정의하는 방법에 대해 기술한다. 그리고 저장된 경보 데이터와 정의된 유사성을 바탕으로 경보 데이터간의 유사성을 분석하여 그 결과를 이용하여 경보 데이터의 분류 모델과 예측 모델을 생성하기 위한 절차에 대해 기술한다

3.1 데이터베이스 스키마 설계

침입 탐지 시스템에 의해 생성되는 경보 데이터를 구조적으로 저장하기 위하여 이 논문에서는 RDBMS를 이용한다. 이는 경보 데이터와 같은 반복적이고 대량의 데이터를 관리하기 위해서는 안정적이고 고속의 RDBMS가 효과적이기 때문이다.

경보 클래스(alert class)는 각 경보의 유일성을 나타내는 Alert ID와 해당 경보의 영향을 나타내는 Impact로 구성된다. Impact는 0~11의 숫자값으로 표현되는데 각 숫자값이 나타내는 의미는 <표 1>과 같다.

경보 클래스의 스키마는 Alert ID와 Impact로 구성된다. 경보클래스의 하위 클래스로서 근원지 클래스(source class), 목적지 클래스(target class), 시간 클래스(time class)가 있다. 근원지 클래스는 침입을 시도하는 주체에 대한 정보를 포함하며 목적지 클래스는 해당 침입의 목적지에 대한 정보를 포함하고 있다. 이 두 클래스는 IP 주소, 포트 번호, 프로토콜로 구성된다.

시간 클래스는 경보가 생성된 시간을 나타내는 생성 시간과 경보를 유발한 침입이 침입 탐지 시스템에 의해 탐지된 시간을 나타내는 탐지 시간으로 구성된다.

〈표 1〉 임팩트 값의 정의

값	표 기 설 명
0	unknown 이벤트영향을 알 수 없거나 정할 수 없음
1	bad-unknown 이벤트의 영향을 알 수 없거나 결정할 수 없을 때, 그러나 바람직하지 않은 경우
2	not-suspicious 이벤트는 어떤 의미로든 의심스럽지 않은 경우
3	attempted-admin 관리자 (super user) 권한 획득 시도
4	successful-admin 관리자 권한 획득 성공
5	attempted-dos 서비스 거부 (denial of service) 시도
6	successful-dos 서비스 거부 성공
7	attempted-recon 조사(reconnaissance probe) 시도
8	successful-recon-limited 제한된 범위에서의 성공적인 조사(예, 한 개의 시스템)
9	successful-recon-largescale 대규모 범위의 성공적인 조사(예, 여러 개의 시스템)
10	attempted-user 사용자 수준 권한 획득 시도
11	successful-user 사용자 수준 권한 획득 성공

3.2 클러스터링을 이용한 데이터 추상화

경보 데이터간의 상관관계를 분석하고, 이를 이용하여 유사한 경보 데이터를 그룹화하기 위하여 이 논문에서는 데이터 마이닝 기법 중 클러스터링을 이용한다. 클러스터링에서 개개 데이터 개체간의 유사성은 근접 지수에 의해 정의된다. 이 근접 지수는 두 데이터 개체간의 유사성이나 연관성을 측정할 수 있는 함수이다. 개체간의 유사성을 측정하는 방법에는 여러 가지가 있지만 주로 거리 개념을 이용하여 측정한다. 이 논문에서는 개체간의 유사성을 정의하기 위해서 유클리드 거리 함수를 이용한다. 이는 동일한 속성값들을 가지는 데이터 개체는 유사하다는 가정을 기반으로 한다. n개의 속성을 가지는 데이터 개체 x, y가 주어지고 각각의 속성의 값이 x_i, $y_i(0 \le i \le n)$로 정의될 때 두 개체간의 거리를 추출하기 위한 함수는 아래 식과 같이 정의된다.

$$dis\_inst(x, y) = \sqrt{\sum_{i=0}^{n} (x_i - y_i)^2}$$

저장된 경보 데이터와 정의된 유사도 측정 함수를 이용하여 클러스터링을 수행하기 위한 절차는 두 단계로 이루어진다. 단계 1은 입력 데이터 집합에 대해 클러스터링 기법을 수행할 수 있도록 적당한 처리를 하는 과정이다.

이 과정은 크게 두 가지 작업을 수행한다. 첫 번째는 클러스터링의 효율적인 수행을 위하여 적당한 속성들을 선택하고 필요에 따라 확장된 속성을 추가하는 과정이다. <표 2>는 클러스터링에 사용되는 경보 데이터의 속성들이다. Alert ID는 각 튜플의 유일성을 구분하기 위한 필드이며 클러스터링에는 사용되지 않는다.

〈표 2〉 클러스터링에 사용된 경보의 속성

속성 이름	데이터 타입	설 명
Alert ID	Integer	각 경보 데이터의 유일한 ID
Impact	Integer	경보를 일으키는 이벤트의 영향 평가
Source Port	Integer	경보를 일으키는 이벤트의 근원지의 포트 번호
Source Protocol	String	근원지 측에서 사용되는 프로토콜
Target Port	Integer	경보를 일으키는 이벤트의 목적지의 포트 번호
Target Protocol	String	목적지 측에서 사용되는 프로토콜
PRE Imp Source	Integer	동일 근원지 IP, 포트의 이전 임팩트
PRE Imp Target	Integer	동일 목적지 IP, 포트의 이전 임팩트

단계 1에서 수행되는 두 번째 작업은 입력 데이터의 정규화이다. 시스템이 일반적으로 설계되기 위해서는 임의의 분포를 가지는 데이터 집합에 대해서도 클러스터링의 수행이 가능하여야 한다. 그러나 정량적인 속성값은 주로 특정 단위를 사용하여 그 값이 측정된다. 그러한 속성값은 측정된 단위에 의존적이므로 이 속성값의 측정 단위가 클러스터링 결과에 영향을 미칠 수도 있다. 이러한 문제점을 해결하기 위해 이 논문에서는 원래의 데이터 개체를 직접 클러스터링에 사용하지 않고 데이터 개체의 분포를 이용하여 클러스터링을 수행한다. 어떤 속성 i와 그 속성값의 m개 튜플이 주어졌을 때, 속성 i의 평균값 $avg[i]$과 표준 편차 $std[i]$를 계산하는 식은 다음과 같이 정의된다.

$$avg[i] = \frac{1}{m} \sum_{j=0}^{m} inst[i]_j$$

$$std[i] = \frac{1}{m-1} \sum_{j=0}^{m} \sqrt{(inst[i]_j - avg[i]^2}$$

계산된 평균과 표준 편차를 이용하여, 각각의 데이터 개체의 속성값들, $insi[i]$은 다음 식에 의해 변경된다.

$$inst[i] = \frac{inst[i] - avg[i]}{std[i]}$$

단계 2는 단계 1에서 처리된 입력 데이터 집합에 대해 실제 클러스터링을 수행하는 과정이다. 주어진 데이터 집합으로부터 클러스터를 생성하기 위하여 CURE 알고리즘을 이용하였다[7, 8]. 이 알고리즘은 고차원의 데이터의 클러스터링을 지원하는 알고리즘이므로 경보 데이터의 클러스터링에 적당하다. CURE는 최초에 데이터 개체 각각을 분리된 클러스터로 간주하고, 모든 개체들이 사용자가 입력한 k개의 클러스터를 형성할 때까지 거리 함수에 의해 클러스터들을 통합함으로써 클러스터링을 수행하는 상향식의 계층적인 클러스터링 기법이다. CURE는 클러스터의 합병을 위해서 거리를 계산할 때 c개의 대표값을 이용하는데, 이 대표값들은 각 클러스터로부터 클러스터의 모양을 가장 잘 표현할 수 있는 c개의 적절히 분포된 포인트를 선택하여 클러스터의 중심점으로 사용자가 입력한 수축률만큼 축소시켜 구해진 점들이다. CURE에서 두 클러스터 u, v간의 거리, $dis_cluster(u, v)$는 다음 식과 같이 정의된다. 이때 p와 q는 각각의 클러스터의 대표값들이다.

$$dis\_cluster(u, v) = \min_{p \in u, q \in n} dis\_inst(p, q)$$

위의 식에 의해 정의된 클러스터간의 거리는 병합하는 과정에서 클러스터간의 유사도를 판단하는 기준이 된다. 이 단계의 결과로서 우리는 유사한 데이터 개체끼리 그룹화된 몇 개의 데이터 집합, 클러스터를 얻는다.

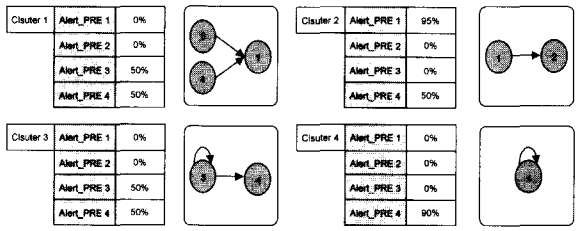
3.3 시퀀스 모델의 추출

이 단계는 생성된 클러스터에 대해 그 생성 원인을 분석함으로써 클러스터간의 순차적인 연관 관계를 추출하는 과정이다. 클러스터간의 연관 관계를 추출하기 위해 이 논문에서는 생성된 클러스터에 포함되는 경보의 이전 경보의 분포를 이용한다. 특정 클러스터에 포함된 경보 데이터의 이전 경보들의 분포를 분석함으로써 해당 클러스터에 포함된 경보 이전에 자주 발생되는 경보를 탐사할 수 있다. 이를 이용하여 특정 클러스터의 이전 경보 클러스터를 정의할 수 있으며, 이전 경보 클러스터로 정의된 클러스터의 다음 경보의 클러스터를 정의할 수 있다. 즉, 두 클러스터 a와 b가 주어졌을 때, 위와 같은 분석 과정을 통해 b의 이전 경보의 클러스터(*cluster_pre*)가 a이면, a의 다음 경보의 클러스터(*cluster_post*)는 b로 정의되고, 두 클러스터의 관계는 a →b로 표현된다. 이러한 각 클러스터간의 순차적인 관계의 분석을 통해 얻을 수 있는 최종 결과는 클러스터로 이루어진 클러스터 시퀀스들이다. <표 3>과 (그림 1)은 클

러스터의 시퀀스를 추출하기 위한 분석 과정을 설명하기 위한 예이다. <표 3>은 클러스터링을 통하여 얻어진 각 클러스터들($cluster_i$)에 대해 각각 이전 경보의 클러스터를 분석한 결과이다. 그림에서 $cluster_1$에 대해 이전 경보의 클러스터는 $cluster_3$, $cluster_4$이다.

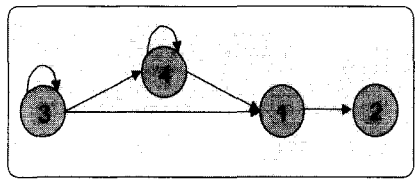
〈표 3〉 클러스터링 결과 테이블

ClusterID	Alert_PRE 1	Alert_PRE 2	Alert_PRE 3	Alert_PRE 4
Clsuter 1	0%	0%	50%	50%
Clsuter 2	95%	0%	0%	0%
Clsuter 3	0%	0%	50%	50%
Clsuter 4	0%	0%	0%	90%



(그림 1) 각 클러스터간의 시퀀스

다시 말해서, $cluster_3$과 $cluster_4$의 다음 정보의 클러스터는 $cluster_1$이다. 이러한 분석의 결과로써 우리는 $cluster_3 \rightarrow cluster_1$, $cluster_4 \rightarrow cluster_1$의 시퀀스를 추출할 수 있다. (그림 1)은 클러스터링의 수행 결과가 <표 3>과 같이 주어졌을 때 클러스터 분석을 통해 얻을 수 있는 클러스터들의 시퀀스를 표현한다. 이렇게 생성된 클러스터의 효율적인 이용을 위하여 이를 통합한다. (그림 2)는 (그림 1)을 이용하여 얻을 수 있는 최종 시퀀스이다.



(그림 2) 최종 클러스터 시퀀스

각각의 경보 데이터의 클러스터링 결과와 시퀀스 분석의 결과를 저장하기 위하여 경보 상관관계 클래스에 Now Cluster ID 속성과 Next Cluster ID 속성을 포함시켜 시퀀스 결과 정보를 관리한다.

3.4 분류 및 예측 모델의 생성

이 과정은 클러스터링을 통해 생성된 클러스터들과 상관관계 분석을 통해 생성된 클러스터들의 시퀀스를 이용하여 룰 데이터베이스를 구축하기 위해 경보의 분류 모델과 예측 모델을 생성하는 과정이다. 이 과정을 통해 구축된 룰을 이용하여 새로운 경보 데이터가 발생했을 경우에, 해당 경보를 자동적으로 적당한 클러스터로 분류하고 다음에 발생할 경보에 대해 예측한다. 분류 모델을 위해 저장해야 할 것들은 입력 데이터의 정규화를 위한 각 속성별 평균 avg[i]과 표준 편차 std[i] (i = 속성의 개수)와 클러스터링의 결과로서 생성되는 각 클러스터들의 대표값 rep[n] (n = 대표값의 개수)이다. 생성된 클러스터의 개수가 m일 때, 총 대표값의 개수는 m×n이다.

새로운 경보 x가 주어지면, 먼저 저장된 평균과 표준 편차를 이용하여 입력 경보 데이터를 x'로 변환한다. 앞에서 설정된 유사도 측정 함수를 이용하여 x'의 가장 가까운 클러스터를 탐색한다. 새로운 분류를 수행하기 위하여 이 논문에서는 결과로 생성된 클러스터의 대표값을 이용한다. 정규화 된 x'의 가장 가까운 클러스터로 선택되고 이에 의해 x의 클러스터를 할당한다. 예측 모델을 생성하기 위해 저장해야 하는 것은 각 클러스터에 대한 이전 경보 데이터의 분포이다. 정의된 이전 경보의 분포를 이용하여 클러스터간의 순차적인 상관관계를 추출할 수 있다. 생성된 분류 모델과 예측 모델을 이용하여 기존에 정의되지 않은 경보나 새로운 타입의 공격에 대한 경보 또한 분류가 가능하며, 향후 발생할 공격에 대한 예측을 시도함으로써 그에 대한 대응 또한 가능하다.

4. 설계 및 구현

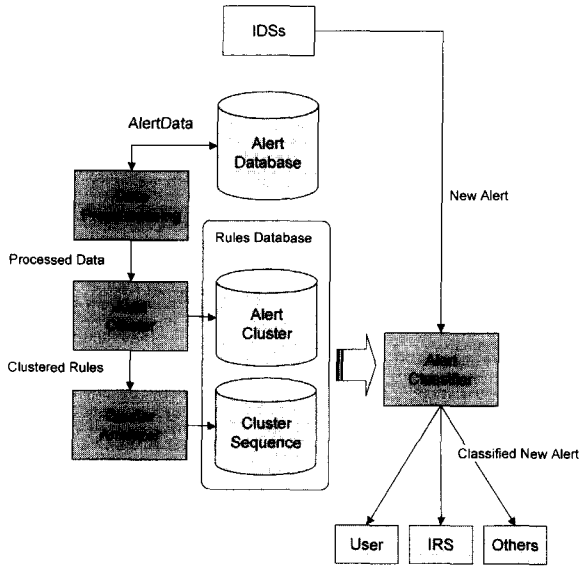
이 장에서는 클러스터링 기법 기반 침입 경보 데이터 유사성 분석 시스템의 설계와 구현에 대하여 기술한다. 경보 데이터 유사성 분석 시스템은 크게 4개의 모듈로 구성되며 상세 구조는 (그림 3)과 같다. 전체적인 흐름은 클러스터링을 수행하기 위한 데이터 전처리 과정과 클러스터링 과정 그리고 클러스터간의 시퀀스 유추과정 등으로 구성되며 각 과정에서 생성된 규칙들은 규칙데이터 베이스에 각각 저장되어 다음 단계에서 활용되어진다.

4.1 설 계

경보 데이터의 유사성을 분석하는 시스템을 구성하는 모듈은 Data Preprocessor, Alert Cluster, Cluster Analyzer 그리고 Alert Classifier이다. (그림 3)은 경보 데이터의 유사성을 분석하기 위한 시스템의 전체 구조를 도식화한 것이다.

Data Preprocessor는 입력된 데이터 집합에 대해 Alert Cluster가 클러스터링을 수행할 수 있도록 전처리를 한다. 여기에서 효율적이고 보다 정확한 클러스터링을 위하여 도메인 지식에 의한 확장 속성을 추가하고 선택된 속성에 대해 정규화를 수행한다. Alert Cluster는 Data Preprocessor에 의해 처리된 데이터에 대해 실제 클러스터링을 수행한

다. 이 모듈의 최종 결과는 그룹화된 데이터의 집합들이다. 그 결과는 룰 데이터베이스에 저장이 되고, 이는 이후에 새로운 경보의 자동적인 분류나 생성된 클러스터 간의 연관 관계 분석에 이용된다. Cluster Analyzer는 클러스터링의 수행을 통해 생성된 클러스터의 생성 원인을 분석한다. 이것에 의해 수행된 결과는 클러스터의 시퀀스로 표현된다. 이를 이용하여 우리는 클러스터간의 연관 관계를 분석할 수 있으며, 특정 경보에 대한 차후 가능한 경보의 집합의 예측에 이용할 수 있다. Alert Classifier는 Alert Cluster에 의해 생성된 클러스터 모델을 이용하여 새로운 경보를 적절한 클러스터로 분류하고, Cluster Analyzer의 결과로서 생성된 시퀀스를 이용하여 차후 발생 가능한 경보들을 추출하는 역할을 수행한다.



(그림 3) 경보 데이터 클러스터링 시스템의 구성

4.2 구 현

경보 데이터에 대해 클러스터링을 수행하기 위해 CURE 알고리즘을 구현하였다. 여기에서 중간 과정의 결과를 저장하기 위해 2개의 데이터 구조를 이용하는데 Heap은 최소 거리를 가지는 2개의 클러스터를 선택하기 위한 것이며, 이를 위하여 입력 데이터 집합은 최초에 가장 가까운 클러스터와 거리를 계산하여 이를 Heap에 저장한다. 또한 KD 트리는 각 클러스터의 대표값을 저장하기 위해서 사용된다. KD 트리는 다차원 데이터를 효율적으로 저장하고 검색할 수 있는 자료 구조이다. 이 알고리즘에서 KD 트리는 2개의 클러스터가 병합될 때, 병합된 클러스터의 가장 가까운 클러스터를 계산하기 위해 사용된다. 입력된 데이터 집합이 Heap과 KD 트리에 저장되면 사용자가 입력한 클러스터의 개수를 만족할 때까지 반복해서 클러스터의 병합을 수행한다. 병합을 수행하는 과정은 아래와 같은 절차에 의해 수행된다.

① Heap에서 가장 가까운 임의의 두 클러스터를 선택한다.
② 선택된 두 클러스터에 포함된 데이터들을 병합한다.
③ 새로운 클러스터의 평균 값을 계산한다.
④ 평균값을 이용하여 새로운 클러스터의 대표 값을 계산한다.
⑤ 새로운 클러스터의 가장 가까운 클러스터를 선택한다.
⑥ 다른 클러스터들의 가장 가까운 클러스터와 그 거리를 갱신한다.
⑦ 기존의 두 클러스터를 삭제한다.
⑧ 새로운 클러스터를 삽입한다.

선택된 두 클러스터의 병합으로 생성되는 새로운 클러스터의 평균, $new.mean$은 아래와 같이 정의된다.

$$new.mean = \frac{|u| \times u.mean + |v| \times v.mean}{|u| + |u|}$$

새롭게 생성된 클러스터의 대표 값을 생성하는 과정은 다음과 같다. 먼저 클러스터에 포함된 데이터 포인트 중에서 대표 값을 계산할 포인트를 선택한다. 최초에는 클러스터의 중심에서 가장 먼 포인트를 선택하고, 그 이후에는 클러스터의 데이터 포인트 중에서 먼저 선택된 포인트와 가장 먼 포인트를 선택한다. 이렇게 선택된 데이터 포인트들은 사용자가 입력한 수축률에 의해 클러스터의 중심으로 수축하여 그 클러스터의 대표 값으로 사용된다.

새로 생성된 클러스터의 가장 가까운 클러스터는 다른 클러스터와의 거리를 계산하고 이를 반복적으로 수행함으로써 계산된다. 새롭게 생성된 클러스터를 제외한 다른 클러스터의 가장 가까운 클러스터를 좀더 효율적으로 계산하기 위해 클러스터를 두 그룹으로 나눈다. 첫 번째 경우는 다른 임의의 클러스터의 가장 가까운 클러스터가 병합된 두 클러스터 중 하나인 경우이다. 두 번째 경우는 임의의 클러스터와 그 클러스터의 가장 가까운 클러스터와의 거리가 임의의 클러스터와 새롭게 생성된 클러스터와의 거리보다 큰 경우이다. 이 경우는 임의의 클러스터의 가장 가까운 클러스터를 새로운 클러스터로 갱신한다. 첫 번째 경우는 다시 임의의 클러스터와 기존의 가장 가까운 클러스터와의 거리와 새로운 클러스터와의 거리에 따라 다시 두 개의 경우로 나누어진다. 임의의 클러스터와 새로운 클러스터와의 거리가 기존의 거리보다 작은 경우에는 임의의 클러스터의 가장 가까운 클러스터를 새로운 클러스터로 갱신한다. 반대의 경우에는 임의의 클러스터의 가장 가까운 클러스터를 다시 계산하여야 한다.

Cluster Analyzer는 Alert Cluster에 의해 생성된 클러스터들의 상관관계를 분석한다. 그 절차는 아래와 같이 수행

된다.

① $cluster_i$에 포함된 각 경보 데이터의 이전 경보 데이터를 추출한다.
② 추출된 이전 경보 데이터가 포함된 클러스터를 탐색한다.
③ ②에서 추출된 클러스터를 바탕으로 $cluster_i_pre[j]$를 정의한다.
④ 각 $cluster_i_pre[j]$의 다음 경보 클러스터로서 $cluster_i$로 할당한다.
⑤ 생성된 시퀀스를 병합하여 최종 시퀀스를 추출한다.

Alert Classifier는 Alert Cluster에 의해 생성된 클러스터 모델을 이용하여 새로운 경보를 적절한 클래스로 분류하고, Cluster Analyzer에 의해 생성된 클러스터 시퀀스를 이용하여 향후 발생할 수 있는 경보의 클러스터를 다음과 같은 절차로 탐색한다.

① x를 입력 데이터 집합의 평균과 표준 편차에 기반하여 x'로 변환한다.
② 각 클러스터와 x'와의 거리를 구한다.
③ 얻어진 거리 중 가장 작은 값을 가지는 클러스터 $cluster_i$를 선택하고 이를 x의 클러스터로 선택한다.
④ 선택된 $cluster_i$를 최종 시퀀스에서 탐색하고, $cluster_i\_post$ 얻는다.

5. 실험 및 평가

이 장에서는 구현된 시스템에 대해 클러스터링의 성능에 대한 실험과 클러스터의 시퀀스를 추출하기 위한 실험을 수행하고 그 결과에 대해 설명한다.

5.1 실험 환경

구현 환경은 Compac Server에서 JAVA와 Pro*C로 구현하였다. 실험한 플랫폼은 Linux 7.1와 Solaris 7에서 수행하였으며, DBMS는 Oracle 8.1.7을 사용하였다.

5.2 실험 방법 및 데이터의 특성

이 논문에서 제안된 방법에 대해 두 가지 측면에 대해 평가를 수행한다. 첫 번째는 구현된 시스템의 클러스터링 성능을 평가하기 위한 실험이다. 이 실험은 구현된 시스템에 의해 생성되는 각 클러스터의 정확도를 평가하는 것이다. 두 번째는 생성된 클러스터에 대해 각 클러스터의 이전 클러스터를 정의하고 이를 기반으로 클러스터의 시퀀스를 생성할 수 있는지의 여부를 평가하기 위한 실험이다.

실험을 위해 사용한 실험 데이터는 KDD Cup 1999 데이터 집합이다[9]. 이 데이터 집합은 DARPA 1998를 이용하여 몇 가지 속성을 추가하여 생성한 데이터 집합이다. DARPA 1998의 트레이닝 데이터는 7주간의 네트워크 트래픽으로 구성된 TCP Dump 데이터이다[10]. 이 데이터 집합은 약 5,000,000개의 데이터 인스턴스로 구성되어 있으며, 네트워크 환경 상에서 가능한 다양한 형태의 침입을 포함하고 있다. 또한 테스트 데이터 집합은 약 2,000,000개의 데이터 인스턴스로 구성되어 있으며, 2주간의 네트워크 트래픽을 기반으로 생성된 데이터 집합이다. 각 데이터 인스턴스는 정상 행위와 각 공격 행위 타입이 명시되어 있다. 트레이닝 데이터 집합에 포함된 공격 타입은 서비스 거부 공격(DOS), 원격지에서의 인가되지 않은 접근(R2L), 슈퍼유저나 루트로의 인가되지 않은 접근(U2R), 취약점 탐사 공격(Probing)이다.

이 논문의 목적은 침입 탐지 시스템의 탐지 결과인 경보 데이터를 분석하기 위해 클러스터링을 수행하는 것이므로, 데이터 집합에서 침입으로 명시된 데이터만 추출하여 실험에 사용하였다. 또한 이 시스템은 클러스터링을 이용한 그룹화를 미리 분류되지 않은 데이터에 적용하여 해당 데이터들을 분류할 수 있는 모델을 생성하는 것이므로, 이 실험에서는 클러스터링 수행 시에 데이터의 미리 표기되어 있는 공격 타입의 레이블은 참조하지 않았다.

5.3 클러스터링 성능

입력 데이터에 대해 클러스터링을 수행하기 위해서는 먼저 사용자 입력 변수를 결정하여야 한다. 이 시스템에는 사용자가 입력하여야 하는 변수가 2개 있다. 선택된 포인터를 대표 값으로 변환하기 위한 수축률과 클러스터의 대표 값의 개수이다. 실험을 위한 수축률과 대표 값의 개수를 선택하기 위하여 우리는 임의로 선택된 10%의 트레이닝 데이터 셋에 대해 클러스터링을 수행하였다.

결정된 입력 변수와 전체 트레이닝 데이터 집합을 이용하여 클러스터를 생성한 후, 우리는 트레이닝 데이터 집합에 포함되지 않은 새로운 데이터 집합을 이용하여 생성된 분류 모델의 정확도에 대한 실험을 수행하였다. 실험을 위한 입력 데이터 집합은 KDD Cup 1999에 포함되어 있는 데이터 집합으로써 트레이닝 데이터 집합과는 달리 레이블이 되어 있지 않는 데이터 집합이다. 테스트 데이터 집합의 공격 타입의 분포는 <표 5>와 같다.

〈표 5〉 테스트 데이터의 구성

공격 타입	비 율
DOS	73.90%
R2L	5.20%
U2R	0.07%
Probing	1.34%

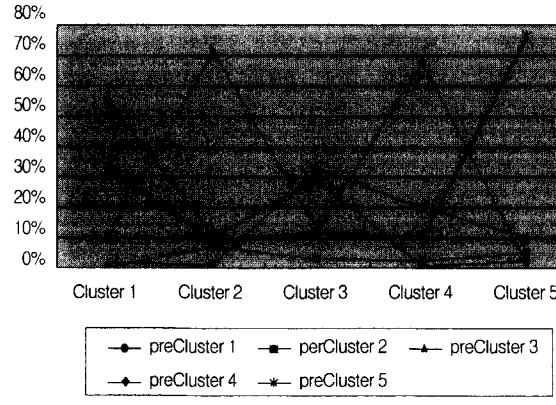
〈표 6〉 테스트 데이터의 분류 결과

공격 타입	클러스터링 정확도
DOS	98.34%
R2L	47.52%
U2R	51.37%
Probing	83.84%

트레이닝 데이터 집합을 이용하여 형성한 모델에 대해 테스트 데이터 집합을 이용하여 실험한 결과는 <표 6>과 같다. <표 6>에 나타나 있는 것처럼 테스트 데이터에 대해서 트레이닝 데이터 집합에 비교적 많이 분포한 클러스터인 DOS, Probing 같은 공격 타입의 경우에는 정확하게 클러스터를 할당하였다. 그러나 분포가 작은 R2L, U2R 공격 타입은 클러스터링 정확도가 다소 떨어졌다. 이처럼 초기 클러스터링 모델을 설정하는 입력 데이터 집합이 다른 요소에 비해 새로운 데이터의 클러스터링 결과에 많은 영향을 미쳤다.

5.4 클러스터링 시퀀스 분석

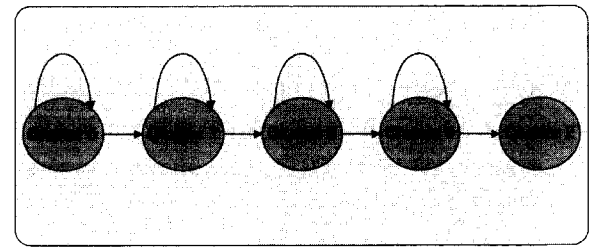
이 실험은 생성된 클러스터에 대해 각 클러스터의 이전 클러스터를 정의하고 이를 기반으로 클러스터의 시퀀스를 생성할 수 있는지의 여부를 평가하기 위한 실험이다. 입력 데이터 집합은 snort에 의해 생성된 실제 경보 데이터를 이용하였으며 사용자 정의 변수는 앞의 실험에 의해 구하여진 값을 사용하였다. 입력 데이터는 약 2시간의 시뮬레이션에 의해 생성된 데이터로서 약 15,000개의 데이터 인스턴스로 구성되어 있다. 속성값은 각 클러스터의 중심값을 나타낸다. 클러스터링 결과를 바탕으로 하여 각 클러스터의 이전 경보 데이터의 분포를 분석하였다. 분석된 결과는 (그림 4)와 같다. (그림 4)의 그래프를 보면 cluster 4에 대한 이전클러스터를 보면 preCluster3의 비율이 가장 높다. 그러므로 Cluster4의 precluster는 Cluster3이 된다.



(그림 4) 클러스터별 이전 경보데이터의 분류

(그림 4)의 이전 클러스터에 따른 시퀀스 분석된 결과를 바탕으로 추출할 수 있는 각 클러스터간의 시퀀스는 (그림 5)와 같다.

(그림 5)에서 원형은 각 클러스터를 나타내며, 화살표는 공격의 진행 방향을 나타낸다. 예를 들면, 새로운 경보가 들어오고 그 경보가 Cluster 4에 분류된다면 이후 발생할 경보 데이터는 Cluster 2에 속하는 것이라는 것을 예측할 수 있게 해준다. 이와 같은 클러스터의 시퀀스를 추출함으로써 특정 클러스터에 포함된 경보 이후에 가능한 경보의 그룹을 알 수 있다.



(그림 5) 클러스터의 시퀀스

6. 결 론

이 논문에서는 침입 탐지 시스템의 탐지 효율을 높이기 위해 데이터 마이닝의 클러스터링 기법을 이용하여 경보 데이터를 그룹화하고 그 결과를 이용하여 경보 데이터의 상관관계를 분석하는 방법을 제안하였다. 즉, 클러스터링 기법을 이용하여 경보 데이터를 사용자가 원하는 개수의 그룹으로 분류할 수 있게 하였으며, 생성된 클러스터 모델을 이용하여 새로운 경보가 들어오면 적당한 클러스터로 분류할 수 있도록 하였다. 또한, 결과 클러스터의 생성 원인이 되는 이전의 경보의 분포 데이터를 저장 관리하여 클러스터간의 시퀀스를 생성하였고, 생성된 각각의 클러스터 시퀀스를 통합하여 클러스터들의 시퀀스를 추출하여 발생한 경보 이후의 향후 발생 가능한 경보 타입을 예측하기 위한 방법을 제공하였다.

클러스터링 알고리즘은 경보 데이터의 특성을 고려하여 다차원의 속성을 가지는 데이터 집합에 대해서도 클러스터링이 가능한 CURE 알고리즘을 확장 구현하였다. 제안된 방법과 구현된 시스템을 평가하기 위해 KDD Cup 1999 데이터 집합에 대해 클러스터링을 수행함으로써, 구현된 클러스터링의 성능을 실험하였으며, 클러스터들의 시퀀스 생성 여부를 실험하였다. 실험을 통하여 많은 양의 데이터에 대한 클러스터링 성능이 우수하다는 결과를 얻었으며 또한 클러스터의 시퀀스 생성도 유도할 수 있었다. 클러스터 시퀀스 생성으로 경보데이터의 분류와 다음경보의 예측이 가능하다는 것은 향후 경보데이터 이후에 가능한 공격에 대한 추측을 할 수 있다는 것으로 해석 가능하다. 그러나 클러스터의

시퀀스 생성 이후에 고 수준의 의미로 변환하여 제공하는 작업이 필요하다.

이 논문에서 제안한 클러스터링을 이용한 경보 데이터의 분석 방법은 다음과 같은 장점을 가진다. 먼저, 데이터간의 유사성을 이용한 경보 데이터의 그룹화를 통해 생성된 모델을 이용하여 새로운 경보 데이터에 대한 분류를 자동화할 수 있다. 이것은 과거에 탐지된 공격의 형태뿐만 아니라 새로운 혹은 변형된 경보의 분류나 분석에도 이용할 수 있다. 두 번째로 생성된 클러스터의 생성 원인의 분석을 이용한 클러스터간의 시퀀스의 추출을 통해 사용자가 공격의 순차적인 구조나 그 이면에 감추어진 전략을 이해하는데 도움을 주며, 현재의 경보 이후에 발생 가능한 경보들을 예측할 수 있으므로 이들을 필요로 하는 보안 분야에 적용할 수 있다.

참 고 문 헌

[1] A. Valdes and K. Skinner, "Probabilistic alert correlation," In Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID 2001), pp. 54-68, 2001.

[2] S. Staniford, J. A. Hoagland and J. M. McAlerney, "Practical automated detection of stealthy portscans," To appear in Journal of Computer Security, 2000.

[3] H. Debar and A. Wespi, "Aggregation and correlation of intrusion-detection alerts," In Recent Advances in Intrusion Detection, number 2212 in Lecture Notes in Computer Science, pp.85-103, 2001.

[4] O. Dain and R. K. Cunningham, "Fusing a heterogeneous alert stream into scenarios," In Proceedings of the 2001 ACM Workshop on Data Mining for Security Applications, pp.1-13, Nov., 2001.

[5] Fred Cuppens, "Managing Alerts in a Multi-Intrusion Detection Environment," In Proceedings of the third International Symposium on Recent Advances in Intrusion Detection (RAID 2000), Toulouse, France, 2000.

[6] Periklis Andritsos, "Data Clustering Techniques," Qualifying Oral Examination Paper, 2001.

[7] Sudipto Guha, Rajeev Rastogi and Kyuseok Shim, "CURE : An Efficient Clustering Algorithm for Large Databases," In Proceedings of the International Conference on Management of Data, (SIGMOD), SIGMOD Record, Seattle, WA, USA, 14, ACM Press, Vol.27(2), pp.73-84, Jun., 1998.

[8] Sudipto Guha, Rajeev Rastogi and Kyuseok Shim, "ROCK : A Robust Clustering Algorithm for Categorical Atributes," In Proceedings of the 15th International Confererence on Data Engineering, (ICDE), Sydney, Australia, 2326, IEEE Press, pp.512-521, Mar., 1999.

[9] KDD99 Cup, http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, 1999.

[10] DARPA 1998 intrusion detection evaluation datasets, http://ideval.ll.mit.edu.

[11] D. Curry and H. Debar, "Intrusion detection message exchange format data model and extensible markup language (xml) document type definition," Internet Draft, draft-ietf-idwg-idmef-xml-03.txt, Feb., 2001.

[12] W. Lee, S. J. Stolfo and K. W. Mok, "A Data Mining Framework for Building Intrusion Detection Models," In Proceedings of the third International Symposium on Recent Advances in Intrusion Detection (RAID 1999), 1999.

[13] W. Lee and S. J. Stolfo, "Data mining approaches for intrusion detection," In Proceedings of the 7th USENIX Security Symposium, 1998.

[14] Ho Sung Moon, Eun Hee Kim, Moon Sun Shin, Keun Ho Ryu, Jinoh Kim, "Implementation of Security Policy Server's Alert Analyzer," ICIS, Aug., 2002.

[15] Moon Sun Shin, Ho Sung Moon, Keun Ho Ryu, Ki Young Kim, Jinoh Kim, "Applying Data Mining Techniques to Analyze Alert Data," APWeb03, Xian, China, Apr., 2003.

[16] Myung Jin Lee, Moon Sun Shin, Ho Sung Moon, Keun Ho Ryu, "Design and Implementation of Alert Analyzer with Mining Engine, IDEAL03, HongKong, China, Mar., 2003.

[17] 박상길, 김진오, 장종수, "보안네트워크 프레임워크에서 이기종의 침입 탐지 시스템 연동을 위한 경보데이터 처리", 제19회 한국정보처리학회 춘계학술발표대회논문집, 제10권 제1호, pp.2169-2172.

신 문 선

e-mail : msshin@dblab.chungbuk.ac.kr

1988년 충북대학교 전산통계학과 학사

1997년 충북대학교 전자계산교육 석사

1999년~현재 충북대학교 전자계산학과 박사과정 수료

관심분야 : 시공간 데이터베이스, 데이터 마이닝, 데이터베이스 보안, 침입 탐지 시스템

문 호 성

e-mail : hsmoon@dblab.chungbuk.ac.kr

2001년 충북대학교 컴퓨터공학과 학사

2003년 충북대학교 대학원 전자계산학과 석사

2003년~현재 가림정보기술

관심분야 : 데이터베이스 보안, 네트워크 보안, 데이터 마이닝, 침입 탐지 시스템

류 근 호

e-mail : khryu@dblab.chungbuk.ac.kr

1976년 숭실대학교 전산학과 이학사

1980년 연세대학교 공학대학원 전산전공 공학석사

1988년 연세대학교 대학원 전산전공 공학박사

1976년~1986년 육군군수 지원사 전산실(ROTC장교), 한국전자통신 연구원(연구원), 한국방송통신대 전산학과(조교수)

1989년~1991년 Univ. of Arizona Research Staff (TempIS 연구원, Temporal DB)

1986년~현재 충북대학교 전기전자및컴퓨터공학부 교수

관심분야 : 시간 데이터베이스, 시공간 데이터베이스, Temporal GIS, 객체 및 지식기반 시스템, 지식기반 정보검색 시스템, 데이터마이닝, 데이터베이스 보안 및 Bio-Informatics

장 종 수

e-mail : jsjang@etri.re.kr

1984년 경북대학교 공과대학 전자공학과 학사

1986년 경북대학교 공과대학 전자공학과 석사

2000년 충북대학교 대학원 컴퓨터 공학과 박사

1989~현재 한국전자통신연구원 책임연구원

네트워크 정보보호 연구본부 보안 게이트웨이 연구팀 팀장

관심분야 : Network Security, Active Security, Biometry