제19회 한국정보처리학회 춘계학술발표대회 논문집 제10권 제1호 (2003.5)

시간연관규칙과 분류규칙을 이용한 비정상행위 탐지 기법

이헌규*, 이양우*, 김룡*, 서성보*, 류근호*, 박진수**
충북대학교 데이터베이스연구실*, 청주대학교 정보통신공학부**
e-mail : {hglee, sbseo, khryu}*@dblab.chungbuk.ac.kr
parkjs**@chongju.ac.kr

Anomaly Detection using Temporal Association Rules and Classification

Hohn Gyu Lee*, Yang Woo Lee*, Lyong Kim*, Sung Bo Seo*, Keun Ho Ryu*, Jin Soo Park**
*Database Laboratory, Chungbuk National University
**School of Information & Communication, Chongju University

요 약

점차 네트워크상의 침입 시도가 증가되고 다변화되어 침입탐지에 많은 어려움을 주고 있다. 시스템에 새로운 침입에 대한 탐지능력과 다량의 감사데이터의 효율적인 분석을 위해 데이터마이닝 기법이 적용된다. 침입탐지 방법 중 비정상행위 탐지는 모델링된 정상행위에서 벗어나는 행위들을 공격행위로 간주하는 기법이다. 비정상행위 탐지에서 정상행위 모델링을 하기 위해 연관규칙이나 빈발에피소드가 적용되었다. 그러나 이러한 기법들에서는 시간요소를 배제하거나 패턴들의 발생순서만을 다루기 때문에 정확하고 유용한 정보를 제공할 수 없다. 따라서 이 논문에서는 이 문제를 해결할 수 있는 시간연관규칙과 분류규칙을 이용한 비정상행위 탐지 모델을 제안하였다. 즉, 발생되는 패턴의 주기성과 달력표현을 이용, 유용한 시간지식표현을 갖는 시간연관규칙을 이용해 정상행위 프로파일을 생성하였고 이 프로파일에 의해 비정상행위로 간주되는 규칙들을 발견하고 보다 정확한 비정상행위 판별 여부를 결정하기 위해서 분류기법을 적용하였다.

1. 서 론[1)]

네트워크 상에서의 침입 시도는 점점 증가되고 다변화되고 있으며, 악의적인 사용자들에 의한 독창적이고 새로운 침입 방식의 개발은 침입 탐지에 대한 어려움을 증가시키고 있다. 침입탐지 시스템의 탐지방법은 오용탐지(*misuse detection*)와 비정상행위탐지(*anomaly detection*) 방법으로 나눌 수 있다[1]. 오용탐지는 이미 알려진 침입 행위를 이용하여 규칙을 생성한 후, 입력 데이터와 규칙이 일치하는 여부에 따라 침입으로 판정한다. 오용탐지 기법은 공격패턴 정보를 가지고 있으므로 정상행위를 공격행위로 간주하는 오류(*false-positive error*)가 낮은 대신 알려지지 않은 새로운 공격은 탐지 할 수 없는 단점을 가지고 있다. 비정상행위탐지는 다양화되는 침입에 대응하기 위해 정상행위의 프로파일(*profile*)을 이용하여 모델링된 정상행위에서 벗어나는 행위 등을 공격행위로 간주하는 탐지기법이다. 그러나 정상행위 프로파일 생성을 위해 다량의 감사데이터를 분석해야 하므로 정확하고 효율적인 분석을 위해 데이터마이닝 기법을 적용하고있다[2]. 지금까지 정상행위를 위한 프로파일 생성에는 빈발 에피소드와 연관규칙 방법이 사용되었다. 그러나 빈발 에피소드는 단순히 데이터의 발생 순서만을 고려하였고 연관규칙에서는 시간요소를 고려하지 않거나 정적인 요소 또는 고정된 시간만을 적용하였다. 실제로 네트워크 연결들에서 발생된 이벤트들의 패턴은 서로 다른 시간단위에 따라서 매우 다르게 나타날 수 있다. 그러므로 시간 요소를 고려하지 않은 지식발견은 정확하고 유용한 지식이라 할 수 없다[11]. 시간요소를 고려한 비정상행위의 탐지를 위해 본 논문에서는 첫째, 비정상행위 탐지를 위해 기존의 연관규칙기법 대신에 다양한 시간 단위에서의 시간 지식을 표현하는 시간연관규칙을 적용한다. 이 규칙에는 시간 표현에서의 주기성과 달력 표현을 포함한 시간 지식을 포함하므로 생성된 시간프로파일은 보다 정확하고 유용한 지식을 표현할 수 있다. 둘째, 시간프로파일을 이용하여 비정상행위로 간주된 규칙들을 발견하고 실제로 비정상행위인지 정상행위인지를 구별하기 위해서 분류기(결정트리)를 이용하여 구분한다. 마지막으로 *tcpdump* 데이터를 이용하여 구현된 탐지 모델에 적용하여 그 결과를 분석한다.

* 이 연구는 한국과학재단 지정 청주대 RRC(정보통신 연구센터)의 지원으로 수행되었음

2. 관련연구

2.1 시간연관규칙 탐사 기법

타임스템프(timestamp)된 트랜잭션에서의 시간연관규칙 탐사기법은 특정 시간간격 동안의 주기적(*cyclic*)인 패턴을 찾아내는 주기적 시간 연관규칙[3]과 달력(*calendar*)으로 표현한 시간 패턴을 가지는 연관규칙을 탐사하는 달력기반 연관규칙 탐사 기법[4]으로 분류할 수 있다.

• 주기적 연관규칙

주기적 패턴이란 시간상에서 정기적으로 발생되는 현상

으로, 예를 들어 매년, 매주, 매일 등, 거의 같은 시기에 주기적으로 발생되는 현상을 찾는 것이다.

• 달력기반 연관규칙

시간 연관규칙을 발견하기 위한 프레임워크로 달력 스키마를 사용하며, 달력 스키마는 시간 단위들의 계층에 의해 결정되어진다. 달력기반 연관규칙의 표현 식은 *(r, e)* 형태이며 연관규칙 *r*은 달력 패턴 *e*에 의해 주어진 각 시간간격 동안 유효한 규칙이다[5].

2.2 시간연관규칙을 이용한 비정상행위 탐지

시간연관규칙을 이용한 비정상행위 탐지 방법은 2.1에서 언급한 시간연관규칙 기법을 이용해 정상행위에 대한 시간지식을 포함한 규칙들을 생성하고 이 규칙들을 시간 프로파일로 만든다. 정상행위 모델을 위해 생성된 시간프로파일은 다량의 감사데이터와 비교한 후 정상행위 패턴에서 벗어나는 규칙들을 찾아 비정상행위로 탐지하는 기법이다[6, 7].

3. 달력기반 시간연관규칙

3.1 시간연관규칙을 위한 달력기반 패턴

시간연관규칙의 표현은 (*r, e*)으로 나타내며 *r*은 발견된 연관규칙이고 *e*는 달력표현식으로써 규칙이 유효한 시간기간을 나타낸다. 달력기반 시간연관규칙을 위해 먼저 다양한 시간단위를 표현하는 달력 스키마를 정의한다.

정의 1. 달력 스키마 $R=(f_n{:}D_n, f_{n-1}{:}D_{n-1}, \ldots, f_1{:}D_1)$이다. 각 속성 f_i는 시간단위이고, D_i는 각 해당 시간단위에서의 도메인을 나타낸다. 스키마 *R*에 대한 달력표현은 $<d_n, d_{n-1}, \ldots, d_1>$으로 나타낸다.

정의 2. 달력표현식에서 주기성을 나타내기 위해서 새로운 문자 "*"를 사용한다. 달력표현에서 "*"의 의미는 해당 도메인의 모든 값을 나타낸다.

예를 들어, 스키마 $R=(Week{:}\{1,..,4\}, Day{:}\{1,...,7\})$가 주어지고 *R*에 대한 달력표현이 $<3, 5>$이라면 그 의미는 "셋째 주 금요일"에 해당하고 $<1, *>$은 "첫째 주의 모든 날"이 된다. 특히, 달력표현에 "*"를 전혀 포함하지 않는 시간표현을 해당 달력 스키마에 대한 기본시간단위라 한다.

3.2 달력기반 시간연관규칙

달력 스키마 *R*이 주어지면 시간연관규칙 (*r, e*)은 *e*에 의해 포함되어지는 타임스탬프된 트랜잭션*(T[e])*에서 최소지지도(S_{min})와 최소신뢰도(C_{min})를 만족하는 규칙이다.

정의 3. 규칙 $<r, e>$이 주어진 시간 기간동안 *f%* 이상을 만족한다면 *r*은 *e*를 만족한다. 이때, *f%*를 최소 발생빈도 (*minimum frequency*) F_{min}이라고 정의한다

위의 예에서 F_{min}의 값을 0.7로 주었을 경우, 규칙 $X \rightarrow Y$은 주어진 시간 기간에서 적어도 70%이상 만족한다면, 규칙 $X \rightarrow Y$은 성립한다.

감사데이터를 위한 시간연관규칙의 탐사에서 기본시간단위(e_0)에서만 유효한 연관규칙은 유용하지 못하다고 가정한다. 왜냐하면 그런 규칙들은 특정 시간간격에 국한되므로 실제로 어떤 반복적인 패턴을 찾을 수 없기 때문이며, 새로운 네트워크 이벤트들에 대한 예측이 불가능하다. 따라서 적어도 "*"를 하나 이상 가지는 시간표현식에서의 규칙들만을 유용한 규칙으로 다룬다.

3.3 빈발 항목집합 발견 알고리즘

감사데이터에 대한 시간연관규칙 적용은 기존의 *Apriori* 알고리즘에 다양한 시간 단위를 지원하도록 확장한다. 그러나 감사데이터의 다량의 값을 가진 다중 속성(근원지 IP, 근원지 포트, 목적지 IP, 서비스인덱스, 목적지 포트 등)들을 다루기 때문에 몇 가지 제약조건이 추가된다. 그 중 생성된 빈발항목집합에 대한 관련된 제약으로는 같은 속성의 두 개의 다른 값을 포함하지 않는다는 것이다. 전체 알고리즘의 수행은 (그림 1)과 같다. 빈발 1-항목집합생성을 제외하고 다음 단계부터 알고리즘은 세 부분으로 나누어진다.

```
1. forall basic time intervals e0 do begin
2.     L1(e0) = {large 1-itemsets in T[e0]}
3.     forall calendar pattern e that covers e0 do
4.         update L1(e) using L1(e0)
5. end
6. for (k=2 ; ∃ a calendar pattern e such that
     L1(e0) != φ ; k++) do begin
7.   forall basic time intervals e0 do begin
8.       generate candidate(Ck(e0)) // Phase 1
9.       forall transaction T∈T[e0] do // Phase 2
10.          subset (Ck(e0), T)
11.      Lk(e0) = {c∈Ck(e0) | c.count ≥ Smin};
       // Phase 3
12.    forall calendar pattern e that covers e0 do
13.        update Lk(e) using Lk(e0)
14.  end
15.  Output (Lk(e), e) for all calendar pattern e.
16. end
```

(그림 1) 빈발 k-항목집합 발견 알고리즘

첫 번째 단계는 기본시간간격에 대한 후보항목집합을 생성한다. 두 번째 단계는 생성된 후보항목에 대한 지지도를 계산해 빈발항목집합을 찾는다. 마지막 단계는 기본시간간격을 포함하는 모든 달력패턴 *e*에 대한 빈발항목집합들을 갱신한다. 첫 번째 단계의 후보항목집합 생성 시 기본시간간격에서만 빈발한 항목집합은 무의미함으로 "*"를 포함하지 않는 달력표현에 대한 후보항목집합은 제거된다. 즉, 기본시간단위에서만 빈발한 후보항목집합들을 줄일 수 있는 함수, $C_k(e_0) = \bigcup_{e \text{ covers } e_0} aprioriGen(L_{k-1}(e) \cap L_{k-1}(e_0))$을 사용한다. 그리고 최소 빈발도 F_{min}가 1(100%)일 경우에는 $L_{k-1}(e)$가 $L_{k-1}(e_0)$의 부분집합이므로 후보항목생성에 $C_k(e_0) = \bigcup_{e_1 \text{ covers } e_0} aprioriGen(L_{k-1}(e_1))$을 사용한다.

생성된 후보항목집합에 대해 다시 *pruning*이 적용될 수 있다. 만약 후보항목집합들이 e_0에서 빈발하더라도 달력패턴 *e*에 대해 빈발하게 되어질 수 없다면 생성된 후보항목집합은 다음 식에 의해 제거된다.

$C_k(e_0) = C_k(e_0) \cap (\bigcup_{e \text{ covers } e_0} L_k(e))$, 여기서 모든 $L_k(e)$는 적어도 전에 한번 이상 갱신되어진 빈발항목집합이다.

알고리즘의 마지막 갱신단계에서는 e_0에서 빈발한 항목집합들을 e_0를 포함하는 달력패턴 *e*에 대해 갱신한다. 즉, $L_k(e_0)$가 $L_k(e)$로 갱신되어질 때, $L_k(e)$안의 항목집합들에 대해 카운트를 1씩 증가시킨다 $L_k(e)$가 갱신되어진

다음 $L_k(e)$의 각 빈발항목집합들에 대해 최소빈발도를 만족하지 못하는 항목집합들은 제거된다. 예를 들어, 전체 e_0의 수를 N개라하고, $L_k(e)$가 n번 갱신되었다면 $L_k(e)$안의 항목집합의 카운터가 $c_update + (N-n) \geq F_{min} \cdot N$를 만족하지 못하면 $L_k(e)$에서 제거된다. (그림 2)는 갱신과정의 한 예를 보여준다(N=5, n=3, F_{min}=0.8).

$L_2(<*,3>)$ Before update	$L_2(<2,3>)$	$L_2(<*,3>)$ After update
{A,B}, c_update=2	{A,B}	{A,B}, c_update=3
{A,C}, c_update=1	{A,C}	{A,C}, c_update=2
{A,D}, c_update=1		~~{A,D}, c_update=1~~
{B,C}, c_update=2	{B,C}	{B,C}, c_update=3
	{B,D}	~~{B,D}, c_update=1~~

(그림 2) $L_2(<*, 3>)$에서의 빈발항목집합 갱신과정

4. 비정상행위 탐지를 위한 지식탐사 기법

비정상행위 탐지는 시간연관규칙과 분류규칙을 사용하여 *tcpdump* 데이터를 분석함으로서 비정상행위 판정 여부를 결정한다. 전체 수행 단계는 크게 두 부분으로 구성된다. 먼저 정상행위로만 구성된 트랜잭션에서 시간연관규칙을 이용해 정상행위 모델 프로파일을 생성한다. 생성된 프로파일은 시간지식을 포함한 연관규칙들로 구성된다. 그러나 실제로, 시간프로파일 생성을 위해서 시간연관규칙들 보다 오히려 빈발항목집합들을 사용한다. 따라서 빈발항목집합들과 시간연관규칙은 교체되어 사용될 수 있다. 다음 단계는 새로운 데이터에서 생성한 시간연관규칙을 정상행위 시간프로파일과 비교 후, 프로파일에 없는 규칙을 비정상행위로 판정한다. 이 경우 정상행위임에도 불구하고 규칙과 일치하지 않으면 비정상행위로 판정되는 거짓 탐지율(*false positive*)이 높아진다. 그러므로 이러한 문제점을 해결하기 위해 비정상행위로 간주되어진 규칙들에 대해 결정트리를 이용해 *false alarms, known attacks, unknown*의 3 클래스로 분류한다.

4.1 시간프로파일과 분류기 생성

tcpdump 데이터로 연관규칙을 적용하기 위해 관련 속성을 추출하여 트랜잭션집합을 생성한다. 전처리 과정을 거친 *tcpdump* 데이터의 테이블 스키마는 다음과 같다.

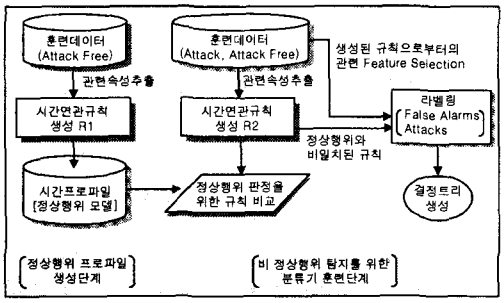
$$R(T_s, SrcIP, SrcPort, DstIP, DstPort)$$

또한 3.3절의 알고리즘 적용 후 의미 있는 규칙들만을 생성하기 위해서 *tcpdump* 데이터 속성 분석결과 생성될 빈발항목집합들을 <표1>과 같이 제한한다. 예를 들어, <SrcIP →ScrPort>와 같은 규칙은 네트워크 연결 이벤트 대한 규칙으로써 무의미하다.

<표 1> 생성될 빈발항목집합들의 형태

Large Itemsets
1. SrcIP, DstIP
2. SrcIP, DstPort
3. SrcIP, SrcPort, DstIP
4. SrcIP, SrcPort, DstPort
5. SrcIP, DstIP, DstPort
6. SrcIP, SrcPort, DstIP, DstPort

훈련데이터를 이용한 시간프로파일과 분류기 생성단계는 (그림 3)의 두 과정을 거친다.



(그림 3) 시간프로파일과 분류기 생성 단계

□ 정상행위모델 시간 프로파일 생성단계

(1) *tcpdump* 데이터에서 공격이 없는 부분만 훈련데이터 집합으로 생성한다.

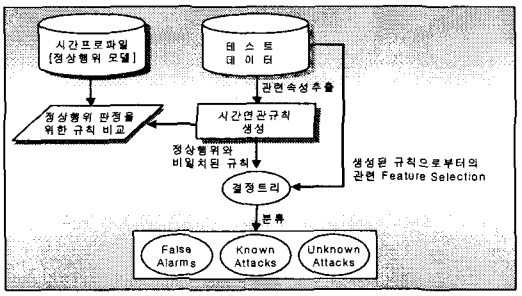
(2) (1)의 훈련데이터에서 마이닝 수행을 위한 관련속성을 추출하고 <표 1>형태의 빈발항목집합들을 생성하여 정상행위 모델의 시간프로파일로 저장한다.

□ 비정상행위 탐지를 위한 분류기 생성단계

(1) 새로운 훈련데이터에서 관련속성 추출 후 시간연관규칙을 생성한다.

(2) 생성된 시간연관규칙의 시간을 포함하는 정상행위 모델의 시간프로파일과 정상행위 판정을 위해 규칙들을 비교한다.

(3) 시간프로파일과 일치하지 않는 규칙들에 대해 비정상행위로 간주하고 훈련데이터에서 관련 *instance vector*들을 분류기를 훈련시키기 위해서 사용되어진다. 기본적으로, 분류기의 *feature vector*들은 연관규칙들로부터 나온 해당 속성들에 관련된다. 훈련데이터에 의한 시간프로파일과 분류기를 생성하고 나면 (그림 4)와 같은 과정을 거쳐 실제 실험 데이터에 대한 비정상행위 판정을 한다. 수행과정은 비정상행위 탐지를 위한 분류기 생성과정과 같은 방식으로 진행되며 비정상행위로 간주된 규칙들에 대해 3가지의 클래스로 분류를 한다.



(그림 4) 테스트 데이터를 이용한 비정상행위 탐지 단계

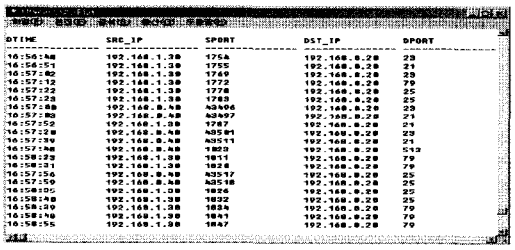
분류 클래스 중 *Unknown Attacks*는 비정상행위로 간주된 규칙들의 이벤트에서 *False alarms*와 *Known Attacks*로 분류되어질 수 없는 이벤트 대한 것은 일반적

분류방식에서 사용되는 "*default label*" 개념을 적용한다. 즉, 시간연관규칙 모듈에 의해 비정상행위로 체크된 이벤트 중 *Known Attacks*로 분류되어질 수 없는 경우에 "*default label*"을 *Unknown attacks* 클래스로 분류한다.

5. 구 현

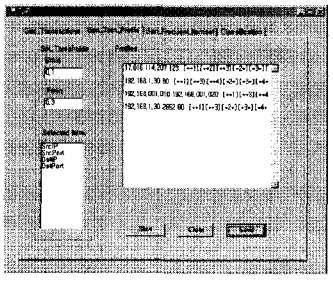
비정상행위 탐지 모델 구현에 사용된 언어는 C# 이고 데이터베이스로 오라클 8i를 사용하였다. 실험 데이터는 *MIT Lincoln Labs*[8]에서 제공하는 7주간의 훈련데이터와 2주간의 테스트 데이터를 사용하였다.

□ 시간프로파일 생성을 위해 공격이 전혀 없는 데이터를 추출하고 시간에 대한 일반화 과정을 거친다. 다음의 (그림 5)는 시간연관규칙에 입력으로 전처리과정을 거친 훈련데이터이다.

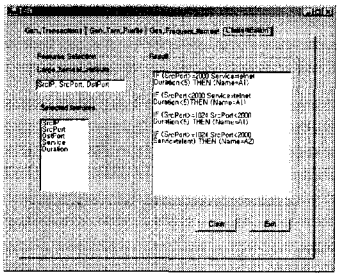


(그림 5) 시간프로파일 생성을 위한 훈련데이터

□ (그림 6)은 주어진 입력데이터에 대해 시간연관규칙을 적용하여 시간프로파일을 생성한다. 최소빈발도를 높게 주었을 때는 규칙생성을 할 수 없으므로 시간에 대해 관련성이 적다는 것을 알 수 있다. (그림 7)은 시간프로파일과 비일치된 실험데이터의 항목들과 *feature selection*으로 얻어진 속성집합에 대한 분류이다.



(그림 6) 시간프로파일 생성



(그림 7) 비정상행위에 대한 분류

6. 결론 및 향후연구

비정상행위 탐지를 위한 기존연구들은 다량의 감사데이터에서 효율적 분석을 통한 침입 여부를 빠르게 판정하기 위해 연관규칙이나 빈발에피소드 기법을 적용한 정상행위 모델 프로파일을 생성하였다. 그러나 프로파일 생성시 감사데이터의 시간 속성을 고려하지 않거나 정적인 요소로써만 고려되었기 때문에 생성된 프로파일에 대한 정확성과 유용성 측면에 문제가 있었다. 이런 문제점을 해결하기 위하여 이 논문에서는 시간연관규칙을 이용한 프로파일 생성 모델을 제안하였다. 이 제안 모델은 생성된 정상행위 프로파일에 주기성 및 달력표현을 지원하며, 그 결과 다양한 시간 단위에서의 시간프로파일이 생성되고 효율적인 비정상행위 탐지가 가능하다. 또한 비정상행위 탐지 기법의 단점인 높은 *false positive error*에 대한 문제점을 해결하기 위해서 비정상행위로 간주된 규칙들에 대해 분류기법을 적용함으로서 더 정확한 분류를 가능하게 하였다.

향후연구로는 기존 분류기법에 유효시간간격과 같은 시간제약조건을 추가하여 확장한 시간분류 기법을 비정상행위 탐지에 적용하는 것이다. 이런 시간 분류규칙은 과거 시점의 규칙이 현재 또는 미래에는 다를 수 있다는 점에서 유용하다.

참고문헌

[1] W. Lee and S. Stolfo, "Data Mining Approaches for Intrusion Detection," In Proc. Of the 7th USENIX Secunity Symposium, 1998.

[2] W. Lee and S. Stolfo, "A Data Mining Framework for Building Intrusion Detection Models," IEEE Symposium on Security and Privacy, 1999.

[3] B. Ozden and S. Ramaswamy, "Cyclic Association Rules," In Proc. Of the 14th International Conference, 1998.

[4] X. Chen and I. Petrounias, "A Framework for Temporal Data Mining," In Proc. Of the 9th International Conference on Database and Expert Systems Applications, 1998.

[5] Y. Li and P. Ning, "Discovering Calendar-based Temporal Association Rules," In Proc. Of the 8th International Symposium on Temporal Representation and Reasoning, 2001.

[6] D. Barbara, J. Couto and N. Wu, "ADAM: Detecting Intrusion by Data Mining," In Proc. Of the 2th IEEE Information Assurance Workshop, 2001.

[7] Y. Li and N. Wu, "Enhancing Profiles for Anomaly Detection Using Time Granularities," In Proc. ACM CCS 2000 workshop on Intrusion Detection Systems, 2000.

[8] MIT Lincoln Laboratories DARPA Intrusion Evaluation Detection. In http://www.ll.mit.edu/IST/ideval/

[9] M. J. Lee, M. S. Shin, K. H. Ryu and K. Y. Kim, "Design and Implementation of Alert Analyzer with Data Mining Engine," *In Proc. Of the 5th International Conference on* Intelligent Data Engineering and Automated Learning, 2003.

[10] M. S. Shin, E. H. Kim, K. H. Ryu and K. Y. Kim, "Data Mining Methods for Alert Correlation Analysis," International Journal of Computer and Information Science(IJCIS), to be appeared in 2003.

[11] 이용준, 서성보, 류근호, 김혜규, "시간간격을 고려한 시간관계 규칙 탐사 기법," 한국정보과학회 논문지 제 28권 3호, 2001.