Journal of Korean
Data & Information Science Society
2007, Vol. 18, No. 2, pp. 315 ~ 326

Design and Evaluation of a Dynamic Anomaly Detection Scheme Considering the Age of User Profiles

Hwa-Ju Lee[1] · Ihn-Han Bae[2]

Abstract

The rapid proliferation of wireless networks and mobile computing applications has changed the landscape of network security. Anomaly detection is a pattern recognition task whose goal is to report the occurrence of abnormal or unknown behavior in a given system being monitored. This paper presents a dynamic anomaly detection scheme that can effectively identify a group of especially harmful internal masqueraders in cellular mobile networks. Our scheme uses the trace data of wireless application layer by a user as feature value. Based on the feature values, the use pattern of a mobile's user can be captured by rough sets, and the abnormal behavior of the mobile can be also detected effectively by applying a roughness membership function with both the age of the user profile and weighted feature values. The performance of our scheme is evaluated by a simulation. Simulation results demonstrate that the anomalies are well detected by the proposed dynamic scheme that considers the age of user profiles.

Keywords: Anomaly Detection, Feature Value, Rough Set, User Profile

1. 서 론

모바일 컴퓨팅 환경의 특징은 상대의 악의적인 공격에 취약하다. 무선 링크의 사용으로 네트워크는 수동적인 엿듣기와 능동적인 간섭에 이르기 까지 공격당하기 쉽다. 공격자가 물리적인 액세스를 획득해야하거나 방화벽과 게이트웨이에서 방어 라인을 통과해야하는 유선 네트워크와 달리 무선 네트워크에서 공격은 모든 위치로부터 발생

1) 경북 경산시 하양읍 금락리 330번지 대구가톨릭대학교 컴퓨터정보통신공학부 박사과정
E-mail : hj2380@lycso.co.kr
2) 교신저자 : 경북 경산시 하양읍 금락리 330번지 대구가톨릭대학교 컴퓨터정보통신공학부 교수
E-mail : ihbae@cu.ac.kr

할 수 있고, 임의의 노드에서 표적이 될 수 있다. 손해는 비밀정보의 누설, 메시지 손상, 노드 위장을 포함할 수 있다 (Zhang 등(2003) 참조).

셀룰러 기반 모바일 무선망에 데이터 서비스 도입으로 사람들은 매일 생활에서 전자 쇼핑과 전자 뱅킹과 같은 중요하고 민감한 일에 셀룰러 전화를 사용하고 있다. 편리하고 인기 있는 새로운 서비스는 중요한 보안 문제가 자연적으로 발생된다. 비록 셀룰러 모바일 망에 많은 인증 프로토콜이 있지만 개방 무선 전송 환경과 모바일 장치의 물리적 취약성으로 보안은 도전할 만한 중요한 분야이다 (Sun 등(2004) 참조).

일반적으로, 시스템을 보호하기 위한 두 가지 보완적인 방법에는 보호와 탐지가 있다. 인증과 암호와 같은 보호 기반 기술은 불법 사용자들의 시스템 진입을 억제하여 공격을 효율적으로 감소시킨다. 그것들은 일반적으로 사용자들이 미리 정의된 보안 정책에 합치하는지를 보장하기 위하여 대칭과 비대칭 메커니즘에 기초한다. 그럼에도 불구하고, 셀룰러 무선망에서 모바일 장치들은 분실과 도난 때문에 물리적으로 안전하지 않다. 매수 방지 하드웨어와 소프트웨어는 대부분 사용자에게 아직 너무 비싸고, 비 보안은 그 장치의 모든 비밀이 악의의 공격자에게 누설된다. 일단 공격자가 장치뿐만 아니라 그 장치와 관계된 모든 비밀을 소유하면, 공격자는 내부 사용자가 되고 전체 네트워크에 엄청난 손실을 발생시킬 수 있다. 이 상황에서 모든 보호 기반 방법들은 도움을 주지 못할 것이다. 따라서 사용자의 정상 행위와 시스템 취약성을 모델하기 위하여 다른 기술을 사용하는 침입 탐지 방법들이 악의의 움직임을 식별하는데 도움을 주기 위하여 설치되었다 (Sun 등(2004) 참조).

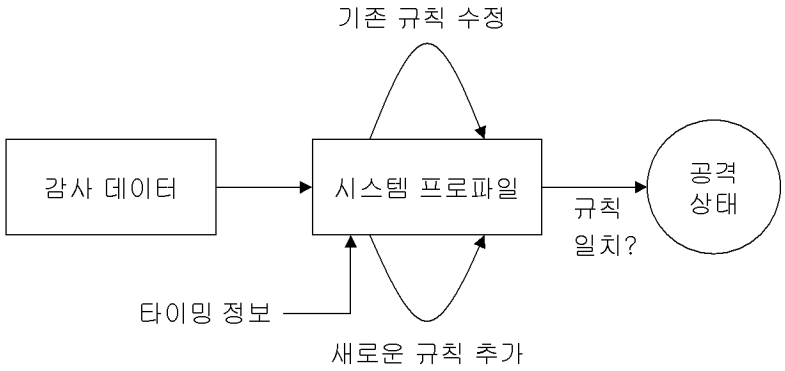
본 논문에서는 러프 셋을 사용하여 정상 프로파일을 구축하고, 사용자 프로파일의 나이와 가중 특징 값을 고려한 러프 소속 함수를 사용하여 비정상 행위를 효율적으로 탐지하는 동적 비정상 행위 탐지 알고리즘을 설계하고, 제안하는 알고리즘의 성능을 모의실험을 통하여 평가한다. 제안하는 알고리즘에서는 모바일 장치의 특징 값으로 사용자에 의해 운행된 셀, 요청 채널의 서비스 종류 그리고 서비스 시간을 사용한다. 침입이 발생했을 때, 합법적인 사용자를 가장한 공격자는 다른 사용 패턴을 가지는 경향이 있다. 그러므로 본 논문에서는 사용 패턴을 비교함으로써 비정상 행위를 효율적으로 탐지한다. 본 논문의 구성은 다음과 같다. 2장에서는 침입 탐지 시스템의 개요와 비정상 행위 탐지에 대한 관련 연구를 살펴보고, 3장에서는 모바일의 특징 값으로부터 정상 패턴을 구축하고 비정상 현상을 탐지하는데 사용되는 러프 집합을 설명하고, 4장에서는 이동 망을 위한 사용자 프로파일 나이와 가중 특징 값을 고려한 러프 집합 기반 동적 비정상 현상 탐지 방법을 제안한다. 5장에서는 모의실험을 통하여 제안하는 비정상 행위 탐지 방법의 성능을 평가한다. 그리고 마지막으로 5장에서 결론과 향후 연구 내용을 기술한다.

2. 관련연구

새로운 자동화된 침입 도구가 매일 출현하기 때문에 컴퓨터 시스템에서 침입 횟수는 증가하고 있다. 편리함을 주는 인기 있는 새로운 서비스는 자연적으로 중요한 보안 문제가 발생된다. 비록 셀룰러 모바일 망에 많은 인증 프로토콜이 있지만, 보안은 개방 무선 전송 환경과 모바일 장치의 물리적 취약성으로 인하여 매우 도전적인 연구이다 (Zhang 등(2003) 참조).

일반적으로 두 가지 침입 탐지 기술에는 오용(misuse) 기반 탐지와 비정상 행위

(anomaly) 기반 탐지가 있다. 오용 기반 탐지 기술은 알려진 공격 서명과 시스템 취약성을 암호화한다. 오용 탐지 방법은 패턴 또는 서명 형식으로 공격을 표현하는 방법들이 있으므로 동일한 공격의 변종들을 탐지할 수 있다. 만일 현재 사용자 활동에 반하는 어떤 패턴을 찾았다면 경고가 발생된다. 오용 탐지 시스템에서 주된 문제는 관련 공격의 모든 가능 변종들을 포함하는 서명을 어떻게 작성할 것인가, 그리고 비침입 활동과 일치하지 않는 서명을 어떻게 작성할 것인가 하는 것이다. 오용 탐지 기술은 시스템 프로파일에 새로운 공격 패턴에 대한 정보가 없기 때문에 새로운 공격을 탐지하는데 비효율적이다. 일반적인 오용 탐지 시스템의 블록 다이어그램은 <그림 1>과 같다 (Sun 등(2004), Vattikonda 등(2003) 참조).

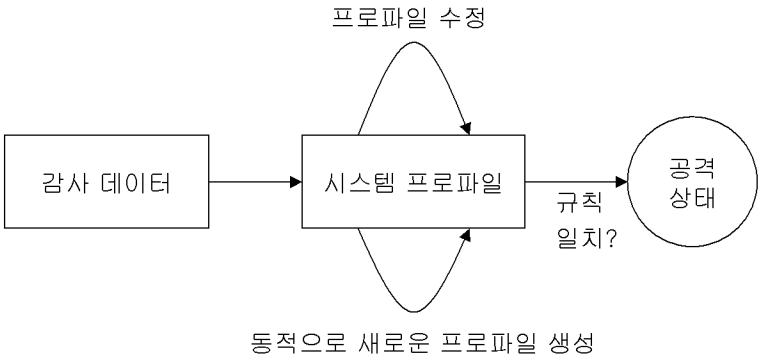


<그림 1> 일반적인 오용 탐지 시스템

비정상 행위 탐지 기법은 모든 침입 활동이 반드시 변칙적이라고 가정한다. 오용 탐지 시스템은 알려진 나쁜 행위의 인식을 시도하지만 비정상 행위 시스템은 나쁜 행위의 보집합(complement) 탐지를 시도한다. 비정상 행위 기반 탐지 기술은 시스템 상태의 정상 프로파일과 사용자 행위를 생성하고 그것들을 현재 움직임과 비교한다. 만일 큰 편차가 관찰되면 알람이 발생된다. 비정상 행위 탐지는 알려지지 않은 공격을 탐지할 수 있다. 만일 침입 활동이 정확하게 동일한 비정상 행위가 되는 대신에 비정상 행위 활동들의 집합과 교차한다면, 흥미 있는 두 가지 가능성이 존재한다.

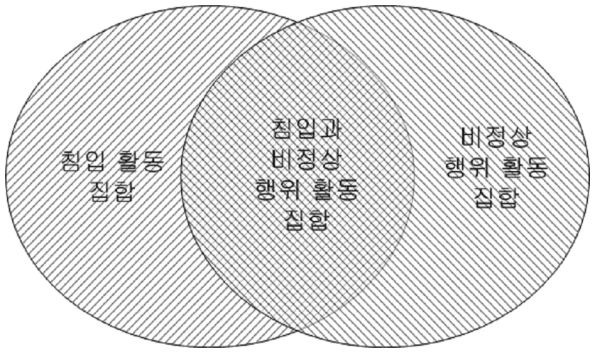
- 침입이 아닌 비정상 행위는 침입으로 플래그 된다.
- 비정상 행위가 아닌 침입 활동은 거짓 부정(false negative)을 일으킨다.

정상 프로파일은 구축하기 일반적으로 매우 어렵다. 따라서 이동 사용자에 대한 정상 프로파일의 구성은 효율적인 침입 탐지 설계에서 중요하다. 일반적인 비정상 행위 탐지 시스템의 블록 다이어그램은 <그림 2>와 같다 (Sun 등(2004), Vattikonda 등(2003) 참조).



<그림 2> 일반적인 비정상 행위 탐지 시스템

<그림 3>은 비정상 행위 활동 집합과 침입 활동 집합을 보여준다. 여기서 교집합이 비정상 행위 활동이고 침입 활동인 부분을 나타낸다. 따라서 최적 비정상 행위 탐지 알고리즘은 비정상 행위 활동 집합과 침입 활동 집합이 동치 집합을 이루게 하여 침입 탐지를 최대화하고 거짓 침입과 거짓 부정을 최소화할 것이다.



<그림 3> 침입 활동 집합과 비정상 행위 활동 집합

Zhang 등(2003)에서 사용자 이동 패턴은 그 사용자에 의해 운행된 셀 ID의 고차 Markov 모델로 기술된다. 이동성 trie에서 데이터를 파스하고 관련 통계 정보를 저장하기 위하여 Ziv-Lempel 데이터 압축 알고리즘을 이용하고, 최근 정상 프로파일 관리를 위해 이동성 trie 갱신에 EWMA(Exponentially Weighted Moving Average)를 적용하였다. Sun 등(2004)에서 셀룰러 모바일 네트워크에서 이동성 기반 비정상 행위 탐지 방법을 제안하였다. 이 방법은 특징 값으로 사용자에 의해 운행된 셀 식별자를 사용하였다. Zhang 등(2000)에서 무선 애드 혹 망을 위한 침입 탐지 에이전트 시스템을 설계하였다. 각 노드의 IDS 에이전트는 독립적으로 실행되고, 국부적 활동을 감시한다. 그것은 국부 추적으로부터 침입을 탐지하고 대응을 시작한다. 만일 비정상 행위가 국부 데이터에서 탐지되거나, 또는 만일 추적이 결정적이 아니고 더 넓은 검색이

정당화되면, 이웃 IDS 에이전트들은 광역 침입 탐지 행위에 협동적으로 참여하는 통합 침입 탐지와 대응 메커니즘을 제안하였다. Kachirski 등(2003)에서는 다수의 망 센서 즉, 패킷 단계, 사용자 단계, 시스템 단계 센서들로부터 검사 데이터를 효율적으로 합병하여 침입에 대해 전체 애드 혹 무선망을 분석하고 침입 억제를 시도하는 분산 협동 침입 탐지 시스템을 제안하였다. Gomez 등(2001)에서는 비정상 행위와 다소의 특정 침입을 탐지하기 위하여 유전 알고리즘을 사용하여 퍼지 분류자를 생성하는 방법을 제안하였다. Lin(1994)에서는 정확한 규칙 대신에 러프 집합의 퍼지 관점에 기초하여 비정상 행위 탐지를 위한 퍼지 규칙을 얻는 소프트 컴퓨팅 방법을 제안하였다. 그리고 Bae 등(2006)에서는 가중 특징 값을 고려한 러프 소속 함수를 사용하여 비정상 행위를 효율적으로 탐지하는 러프 집합 기반 비정상 행위 탐지 방법을 제안하였다.

3. 러프 집합

러프 집합은 부정확하고 불완전한 데이터 분류 문제를 다루는 수학적 기법으로 식별불가능(indiscernible) 객체의 클래스로 구성된 동치 관계를 기본으로 하고, 서로소 범주로 나눈 영역의 분류인 하한 근사와 상한 근사라 부르는 정확한 개념의 쌍에 의한 모호한 개념의 근사화이다. 러프 집합 방법은 그러한 근사에 기초하여 불완전한 데이터를 처리한다. (변증남 등(1999). Pawlak(1991), Jensen 등(2002) 참조)

U를 전체집합이라 부르는 객체들의 유한집합이라 하고, $R \subseteq U \times U$를 U의 동치관계라 한다. 쌍 A=(U, R)을 근사 공간이라 하고, 동치관계 R의 동치 클래스를 A에서 기본집합이라 한다.

원소 $x \in U$에 대해, x를 포함하는 R의 동치 클래스를 $[x]_R$로 표시한다. 각 부분집합 $X \subseteq U$에 대해, X는 식 (1)과 같이 정의되는 A에서의 상한근사와 하한근사에 의해 특징 지워진다.

$$\begin{aligned} \underline{A}X &= x \in U \mid [x]_R \subseteq X \\ \overline{A}X &= x \in U \mid [x]_R \cap X \neq \varnothing \end{aligned} \tag{1}$$

$\underline{A}X$내의 객체들은 R 지식에 기초하여 X의 요소로 확실히 분류될 수 있다. 반면에, $\overline{A}X$내의 객체들은 R 지식에 기초하여 X의 긍정 구성요소로만 분류될 수 있다. 집합 $BN_A X = \overline{A}X - \underline{A}X$를 X의 A-경계 지역이라 하고, A내의 지식에 기초하여 X로 결정적으로 분류할 수 없는 객체들로 구성된다.

러프 집합은 근사 정확성이라 하는 식 (2)의 계수에 의해 수치적으로 기술될 수 있다. 여기서 Card는 집합원의 개수(cardinality)를 나타낸다.

$$\alpha_A(X) = \frac{card \underline{A}X}{card \overline{A}X} \tag{2}$$

분명히 $0 \leq \alpha_A(X) \leq 1$이다. 만일 $\alpha_A(X) = 1$이면, X는 A에 대해서 명백(crisp)하다. 반면에 $\alpha_A(X) < 1$이면, X는 A에 대해서 러프(rough)하다.

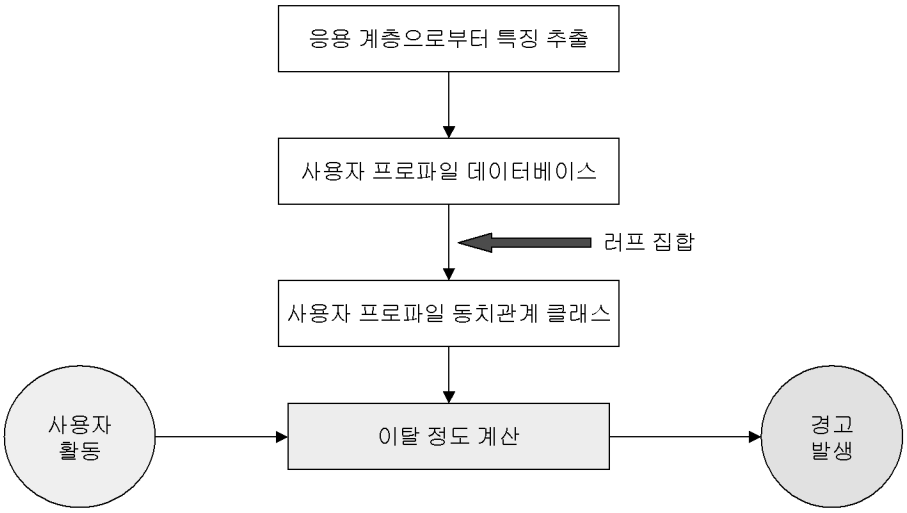
집합 X의 정확성 정도를 나타내기 위하여 다소의 다른 척도가 정의될 수 있다. $\alpha_A(X)$의 변량(variety)을 측정하기 위하여 식 (3)을 사용할 수 있고, X의 A-러프니스라 한다.

$$\rho_A(X) = 1 - \alpha_A(X) \tag{3}$$

정확성에 반대되는 러프니스는 집합 X에 대한 지식 A의 불완전성 정도를 나타낸다.

4. 동적 비정상 행위 탐지 방법

본 논문에서 제안하는 러프 집합 기반 동적 비정상 행위 탐지 방법의 구조는 <그림 4>와 같다.



<그림 4> 러프 집합 기반 비정상 행위 탐지 방법의 구조

먼저 무선 응용 계층으로부터 사용자 활동의 특징을 추출하여 사용자 프로파일 정보 데이터베이스를 구축하고, 러프 집합을 사용하여 그 사용자 프로파일의 동치류를 계산한다. 여기서 무선망 서비스에 처음 가입한 사용자의 프로파일은 그 사용자의 가입 신청서를 기반으로 구축되고, 시간에 따라 최근 사용자 프로파일이 동적으로 유지되어진다. 그리고 사용자 활동에 대한 정보와 그 사용자의 프로파일에 대한 동치류 정보를 기초로 러프 집합을 사용하여 정상 행위로부터 이탈 정도(deviation number)를 계산한다. 여기서 이탈 정도는 현재 사용자 활동이 정상 행위에서 벗어난 편차를 나타낸다. 그 이탈 정도가 시스템에서 설정된 허용 오차인 이탈 임계치보다 크면, 침입 탐지 시스템은 경고 정보를 생성한다.

러프 집합 기반 동적 비정상 행위 탐지 알고리즘은 응용 계층의 특징 값으로 각 각 모바일 사용자가 과거 일정 기간 동안의 그 사용자에 의해 운행된 셀 식별자, 사용자 요청 채널의 서비스 시간 그리고 서비스 종류를 사용한다. 무선 이동 망에서, 프로파

일 정보는 사용자의 개인 정보와 함께 HLR에 저장된다. 우리는 HLR이 안전하고 그 프로파일 정보는 정확하다고 가정한다. 일반적으로, HLR의 중요성 때문에 HLR은 아주 안전한 대책으로 보호되므로 HLR 공격은 매우 어렵다.

관계/뷰 사례는 데이터베이스에서 표현되는 엔티티와 객체의 사용자의 즉시 인식을 나타내는 관계형 데이터베이스의 스냅 샷이다. 프로파일 정보가 관계형 데이터베이스의 스냅샷의 사례이다. 우리의 프로파일 정보는 엔티티 무결성 제한 없이 관계형 데이터베이스의 확장이다. <표 1>은 사용자 프로파일 정보 데이터베이스를 보여준다. 여기서 REQ#, CELL, DUR, CLASS, AGE는 사용자 채널의 요청 번호, 운행된 셀 식별자, 요청 채널의 서비스 시간, 요청 채널의 서비스 종류, 프로파일 데이터의 나이를 각각 나타낸다. 그 프로파일 데이터는 계속해서 생성되고 없어진다. 프로파일 데이터의 나이가 작을수록 새로운 프로파일 데이터이다.

<표 1> 사용자 특징 프로파일 정보 시스템

REQ#	CELL	DUR	CLASS	AGE
1	a	1	α	3
2	a	1	α	3
3	a	2	α	3
4	b	2	β	3
5	b	2	β	3
6	b	2	β	2
7	b	2	β	2
8	b	3	γ	2
9	c	3	γ	2
10	c	3	γ	2
11	a	1	α	1
12	a	1	α	1
13	a	2	α	1
14	b	2	β	1
15	b	3	β	1

표 1의 사용자 특징 프로파일 정보 시스템에서 CLASS 속성을 결정 속성이라 하면, 결정 클래스라 부르는 3가지 동치 클래스를 가진다.

DE1={1, 2, 3, 11, 12, 13}={α}
DE2={4, 5, 6, 7, 14, 15}={β}
DE3={8, 9, 10}={γ}

조건 속성 (CELL, DUR)에 대해, 우리는 조건 클래스라 부르는 5가지 동치 클래스를 가진다.

CE1={1, 2, 11, 12}
CE2={3, 13}
CE3={4, 5, 6, 7, 14}
CE4={8, 15}
CE5={9, 10}

위의 조건 클래스와 결정 클래스를 비교하면, 다음과 같은 포함관계를 얻을 수 있다.

CE1 ⊆ DE1
CE2 ⊆ DE1
CE3 ⊆ DE2
CE5 ⊆ DE3

조건 클래스 CE4와 결정 클래스 DE2 간의 포함 관계는 퍼지 포함으로 표현될 수 있다. 퍼지 포함은 소속 함수의 부등식으로 표현된다. 퍼지 포함이 허용 범위 안에 있는 한 어느 정도 오차를 허용할 것이다. $V_1 = \overline{R}X_1 \cup \overline{R}Y$, $V_2 = \overline{R}X_2 \cup \overline{R}Y$, $W_1 = \overline{R}X_1 \cap \overline{R}Y$ 그리고 $W_2 = \overline{R}X_2 \cap \overline{R}Y$이라 한다. 여기서 X_i와 Y는 각각 조건 속성과 결정 속성을 나타낸다. 퍼지 포함은 본 논문에서 제안한 식 (4)의 러프니스 소속 함수에 의해 계산된다. 여기서 퍼지 포함은 이탈 정도를 의미한다.

$$\rho = \min(1-\alpha(V_1, W_1), 1-\alpha(V_2, W_2)) \tag{4}$$

여기서 $\alpha(V_1, W_1) = \dfrac{\sum_{age=1}^{g}\left[Card(W_1) \cdot (w_{x_1} + w_y) \cdot wa_{age}\right]}{\sum_{age=1}^{g}\left[Card(V_1) \cdot (\max(w_x) + w_y) \cdot wa_{age}\right]}$,

$\alpha(V_2, W_2) = \dfrac{\sum_{age=1}^{g}\left[Card(W_2) \cdot (w_{x_2} + w_y) \cdot wa_{age}\right]}{\sum_{age=1}^{g}\left[Card(V_2) \cdot (\max(w_x) + w_y) \cdot wa_{age}\right]}$이다. 그리고 g와 wa_{age}는 나이 등급의 개수와 나이의 가중치를 각각 나타내고, w_{x_i}와 w_y는 사용자의 i-번째 조건 속성의 가중치와 결정 속성의 가중치를 각각 나타내고, $\max(w_x)$는 조건 속성 중에서 최대 가중치 값을 구하는 함수를 나타낸다.

포함 관계에 있지 않는 CE4와 DE2에 대해, X=CE4={b, 3}, Y=DE2={β}, $w_{cell} = 0.45$, $w_{dur} = 0.25$, $w_{class} = 0.3$, $aw_1 = 1.0$, $aw_2 = 0.5$ 그리고 $aw_3 = 0.1$이라 두면, $\overline{R}X_1$={4, 5, 6, 7, 8, 14, 15}, $\overline{R}X_2$={8, 9, 10, 15}그리고 RY={4, 5, 6, 7, 14, 15}이므로 V_1={4, 5, 6, 7, 8, 14, 15}, V_2={4, 5, 6, 7, 8, 9, 10, 14, 15}, W_1={4, 5, 6, 7, 14, 15} 그리고 W_2={15}이다. 따라서 식 4에 의해 계산된 러프니스 $\rho = \min(0.135, 0.844)$ =0.135이다. 그러므로 CE4와 DE2는 0.135-퍼지 포함 관계가 있다.

$$CE4 \subseteq_{(0.135)} DE2$$

비정상 행위 탐지 시스템의 정상 상태로부터 허용하는 오차(ε)를 0.5로 설정하고, 사용자 활동 (c, 2, β)가 발생한 경우, X={c, 2}, Y={β}라 두면, $\overline{R}X_1$={9, 10}, $\overline{R}X_2$={3, 4, 5, 6, 7, 13, 14} 이고 $\overline{R}Y$={4, 5, 6, 7, 14, 15}이다. 그러므로 사용자 활동의 이탈 정도는 $\rho = \min(1.0, 0.625)$=0.625이다. 따라서 $\rho > \epsilon$이므로 사용자 활동은 비정상 행위로 평가되고 경고 메시지가 생성된다. 반면에 사용자 활동 (b, 3, β)가 발생한 경우, 사용자 활동의 이탈 정도 $\rho = \min(0.103, 0.844)$=0.103이다. 따라서 $\rho \leq \epsilon$이므로 사용자 활동은 정상 행위로 식별된다.

5. 성능 평가

본 논문에서 제안하는 비정상 행위 탐지 방법의 성능을 평가하기 위하여 다음 두 가지 척도를 사용한다.

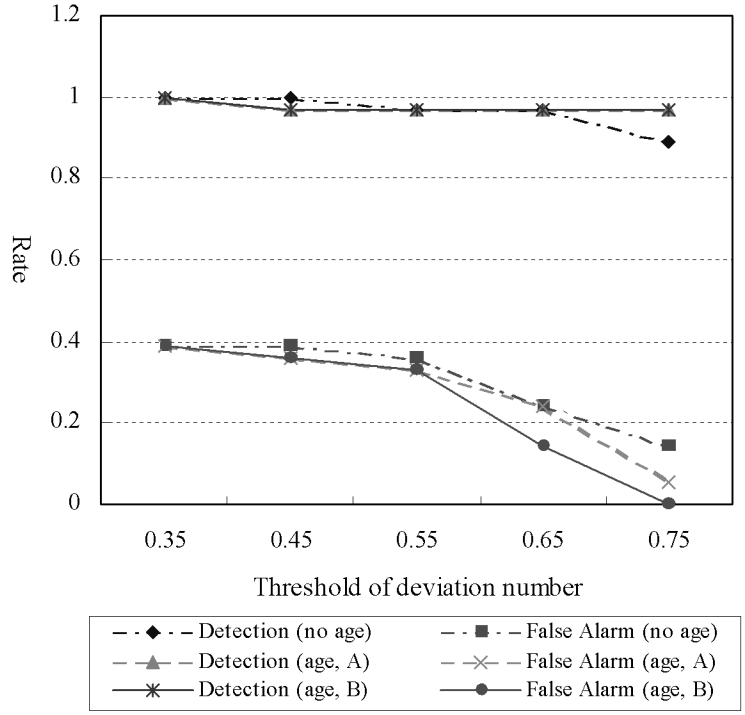
- 탐지율(Detection Rate): 비정상 행위로 측정된다. m′ 비정상 행위에 대하여 n이 비정상인 것으로 탐지되면, 탐지율은 n/m′으로 정의된다.
- 거짓 경고율(False Alarm Rate): 정상 행위로 측정된다. m 정상 행위에 대하여 n이 비정상인 것으로 식별되면 거짓 경고율은 n/m으로 정의된다.

우리는 모의실험을 통하여 이탈 정도에 따른 제안하는 러프 집합 기반 동적 비정상 행위 탐지 방법의 성능을 분석하고 설명한다. 모의실험에서, 나이 1의 경우에 만일 어떤 사용자 활동이 사용자 활동 속성 값들 중에서 두 개의 값이 그 사용자 프로파일 데이터의 특징 값과 일치하는 두 개 이상의 레코드를 가지면, 그 사용자 활동은 정상이라 가정한다. 또한 만일 어떤 사용자 활동이 사용자 활동 속성 값들 중에서 두 개의 값이 그 사용자 프로파일 데이터내의 나이 1의 특징 값과 일치하는 하나의 레코드를 가지고, 그 사용자 활동이 사용자 활동 속성 값들 중에서 두 개의 값이 그 사용자 프로파일 내의 나이 2 또는 나이 3의 특징 값과 일치하는 하나 이상의 레코드를 가지면 역시 정상이라 가정한다, 만일 <표 2>는 모의실험에서 사용된 매개변수와 값을 보여준다. 여기서 사례 A와 사례 B의 차이는 나이 간의 가중치의 차이가 크고 작고 한 것이다.

<표 2> 모의실험 매개변수

매개변수	값	
사용자 활동 횟수	1,000	
가중 특징 값 ($w_{cell}, w_{dur}, w_{class}$)	(0.45, 0.25, 0.3)	
나이 가중치의 사례 (1, 2, 3)	A	(1.0, 0.7, 0.3)
	B	(1.0, 0.5, 0.1)
운행된 셀 ID	random(1, 4)	
서비스 기간의 종류	random(1, 4)	
서비스 클래스의 종류	random(1, 3)	

제안하는 동적 비정상 행위 탐지 방법의 성능은 Bae 등(2006)의 가중 특징 값을 고려한 러프 집합 기반 비정상 행위 탐지 방법의 성능과 비교한다. <그림 5>는 이탈 임계치에 대한 탐지율과 거짓 경고율의 모의실험 결과를 보여준다. 제안하는 동적 비정상 행위 탐지 방법의 탐지율(Detection(age))은 Bae 등(2006)의 탐지율(Detection(no age))과 거의 같은 성능을 보이나 동적 비정상 행위 탐지 방법의 거짓 경고율(False Alarm(age))은 이탈 임계치와 관계없이 Bae 등(2006)의 거짓 경고율(False Alarm(no age)) 보다 우수한 성능을 보인다. 우리의 방법에서, 사례 B(Detection(age, B), False Alarm(age, B))의 성능이 이탈 임계치와 관계없이 사례 A(Detection(age, A), False Alarm(age, B))의 성능 보다 우수하다. 따라서 나이 간의 가중치 차이를 크게 줄수록 더 좋은 성능을 얻을 수 있다는 것을 알 수 있었다. 아울러, 이탈 임계치를 0.75로 설정했을 때, 사례 B의 가중치 나이를 갖는 동적 비정상 행위 탐지 방법이 최적 성능을 갖는다는 것을 확인하였다.



<그림 5> 이탈 허용 오차에 따른 탐지율과 거짓 경고율

본 논문에서 제안하는 동적 비정상 행위 탐지 방법에서는 조건 속성으로 모바일의 이동 패턴을 사용한다. 그러나 정규 이동성을 보이지 않는 택시 운전사와 같은 소수의 사용자들이 있다. 그러한 사용자를 위해서는 사용자 프로파일에서 조건 속성을 선택적으로 사용할 수 있기 때문에 제안하는 방법은 모든 사용자에게 적용할 수 비정상 행위 탐지 방법이다.

6. 결 론

본 논문에서는 무선 이동 망을 위한 러프 집합 기반 동적 비정상 행위 탐지 방법을 제안하고 그것의 성능을 모의실험을 통하여 평가하였다. 제안하는 방법은 특징 값으로 무선 응용 계층의 사용자 활동 정보를 사용하였다. 특징 값은 사용자에 따라 선택적으로 사용할 수 있기 때문에 제안하는 비정상 행위 탐지 방법은 모든 사용자들에게 적용할 수 있다. 모의실험 결과, 사용자 프로파일의 나이를 고려한 동적 비정상 행위 탐지 방법이 나이를 고려하지 않는 정적인 방법 보다 성능이 우수하다는 것을 확인하였다.

향후 연구 내용은 나이를 갖는 사용자 행위의 정확한 이탈 정도를 측정하는 방법, 이탈 임계치를 결정하는 방법, 그리고 제안하는 방법을 무선 애드 혹 네트워크에 적

용하는 것 등이다.

참고 문헌

1. 변증남, 방원철 (1999). 러프집합의 이론과 응용, 청문각.
2. Bae, I. H., Lee, H. J., Lee, K. S. (2006). Design and Evaluation of a Rough Set-Based Anomaly Detection Scheme Considering Weighted Feature Values, *KES 2006*, Part I, LNAI 4251, Springer-Verlag Berlin Heidelberg, 483-489.
3. Gomez, J. and Dasgupta, D. (2001). Evolving Fuzzy Classifiers for Intrusion Detection, *Proceedings of the Workshop on Information Assurance United States Military Academy*, 1150-1161
4. Jensen, R. and Shen, Q. (2002). Fuzzy-Rough Sets for Descriptive Dimensionality Reduction, *Proceedings of the 11th International Conference on Fuzzy Systems*, 29-34.
5. Kachirski, O. and Guha, R. (2003). Effective Intrusion Detection Using Multiple Sensors In Wireless Ad Hoc Networks, *HICSS'03*, 57.1
6. Lin, T. Y. (1994). Anomaly Detection - A Soft Computing Approach, *Proceedings of the 1994 Workshop on New Security Paradigms*, 44-53
7. Pawlak, Z. (1991). *Rough Sets Theoretical Aspects of Reasoning about Data*, Kluwer Academic Pub.
8. Sun, B., Yu, F., Wu K. and Leung, V. C. M. (2004). Mobility-Based Anomaly Detection in Cellular Mobile Networks, *WiSe'04*, 61-69.
9. Vattikonda A., Gampa, R. K., Isukapalli, V. K. and Kakarlapudi V. R. (2003). Intrusion Detection in Wireless Networks, *Department of Computer Science, The University of Kentucky, Term Paper.*
10. Zhang, Y, and Lee, W. (2000). Intrusion Detection in Wireless Ad-Hoc Networks, *MobiCom'2000*, 275-283.
11. Zhang, Y., Lee, W. and Huang, Y-A. (2003). Intrusion Detection Techniques for Mobile Wireless Networks, *ACM/Kluwer Mobile Networks and Applications*, 9(3) 545-556.

[2007년 3월 접수, 2007년 4월 채택]