Journal of the Korean Data & Information Science Society
2010, **21**(6), 1125–1136

한국데이터정보과학회지

모바일 애드-혹 망을 위한 퍼지 비정상 행위 탐지 알고리즘

배인한[1]

[1]대구가톨릭대학교 컴퓨터정보통신공학부

접수 2010년 9월 11일, 수정 2010년 10월 27일, 게재확정 2010년 11월 1일

요 약

최근에 이동 객체 추적 장치로부터 얻어진 추적 스트림에 대한 온라인 비정상 행위 감시에 대한 요구가 증가하고 있다. 제한된 공간 비용 내에서 고속 데이터 처리의 요구사항에 기인하여 이 문제는 흥미를 끌고 있다. 이 논문에서, 우리는 모바일 애드 혹 망에서 모바일 장치의 위성항법장치 로그로부터 이동특징 정보를 계산하여 정상 프로파일을 구축하고, 모바일 장치의 현재 이동 특징 정보와 정상 프로파일내의 이동 특징 정보간의 퍼지 비유사도를 계산한다. 그 계산된 퍼지 비유사도를 기초로 그 모바일 장치의 비정상 행위를 효율적으로 탐지하는 퍼지 비정상 행위 탐지 알고리즘을 제안한다. 그리고 모의실험을 통하여 제안한 알고리즘의 성능을 평가한다.

주요용어: 비정상 행위 탐지, 위성항법장치 데이터, 유사도, 이동 패턴, 퍼지 논리 이론.

1. 서 론

모바일 애드-혹 망 (MANETs, mobile ad-hoc networks)은 모바일 호스트를 위한 무선 통신의 새로운 패러다임이다. 모바일 애드 혹 망에는 모바일 스위칭을 위한 기지국과 같은 고정된 인프라구조가 없고, 서로 전파 범위 내에 있는 노드들은 무선 링크를 통해 직접 통신한다. 그러나 서로 멀리 떨어져 있는 노드들은 메시지 전달을 위해 다른 노드들에 의존하고, 각 노드는 라우터와 호스트로 역할을 할 수 있다. 그리고 노드 이동성은 빈번한 위상 변경을 일으킨다. 통신의 무선 특징과 보안 인프라 구조가 없기 때문에 다소의 보안 문제를 일으킨다 (Rezaul 등, 2006). 모바일 애드 혹 망은 미리 존재하는 인프라 구조와 집중화된 제어가 없기 때문에 WLANs (Wireless Local Area Networks)와 무선 네트워크에서 개발된 일반적인 침입 탐지 알고리즘들은 애드 혹 망에 맞지 않는다.

비정상 행위 탐지는 침입은 정상 행위와 다르고 그러한 차이를 식별함으로써 탐지될 수 있다고 가정한다. 그것은 먼저 일련의 특징 매개변수들과 임계값들로 보호될 시스템의 정상 프로파일을 정의한다. 그리고 실시간 탐지 프로세스에서, 그것은 현재 시스템 상태와 정상 프로파일 간의 차이를 식별하기 위하여 그것들을 비교한다. 미리 정의된 임계값 보다 큰 차이는 그 시스템이 비정상 상태에 있다는 것을 의미한다 (Zhu와 Xiong, 2005).

따라서 본 논문에는 모바일 애드 혹 망에서 모바일 장치의 위성항법장치 (GPS, Global Positioning System) 로그로부터 이동 특징 정보를 계산하여 정상 프로파일을 구축하고, 모바일의 현재 이동 특징 정보와 프로파일내의 정상 이동 특징 정보간의 퍼지 비유사도를 계산한다. 그 계산된 퍼지 비유사도를 기초로 그 모바일 장치의 비정상 행위를 효율적으로 탐지하는 FADA (Fuzzy Anomaly Detection Algorithm)를 제안한다. 그리고 모의실험을 통하여 제안한 알고리즘의 성능을 평가한다.

[1] (712-702) 경북 경산시 하양읍 금락로 5, 대구가톨릭대학교 컴퓨터정보통신공학부, 교수.
E-mail: ihbae@cu.ac.kr

2. 관련연구

2.1. 비정상 행위 탐지

MANET에서 현존하는 IDS (Intrusion Detection System)의 가능한 구조는 독립 IDS, 분산 그리고 협력적 IDS 그리고 계층적 IDS를 포함한다 (Brutch와 Ko, 2003).

- 독립형 (Stand-alone) IDS: 이 구조에서는 각 호스트가 IDS를 가지고 독립적으로 공격을 탐지한다. 노드들 사이에서의 협력은 없고 모든 결정은 지역노드들에 의한다. 이 구조는 충분히 효율적이지는 않지만 모든 노드에서 IDS를 실행 시킬 능력이 없는 환경에서 사용될 수 있다.
- 분산 및 협력 (Distributed & Cooperative) IDS: 이 구조에서는 각 노드가 IDS 에이전트를 가지며 지역 탐지 결정을 한다. 동시에 모든 노드들이 전역 탐지 결정에 참여한다. 이 구조는 플랫 MANET에 적합하다.
- 계층적 (Hierarchical) IDS: 이 구조는 다중 계층 MANET을 위해 설계되었다. 다중 계층 MANET에서는 클러스터 헤드 (CH, Cluster Head) 노드가 클러스터 내의 모든 노드들에 대한 중앙집중식 라우팅을 하며 IDS를 포함한 보안 수단을 지원할 수 있다. 더욱이, CH 노드는 또한 Byzantine CH 노드에 의해 만들어진 가상 백본 라우팅 프로토콜에 대한 공격을 탐지할 수 있는데 이는 MANET에서 매우 중요하다.

Zhang과 Lee (2000)은 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 요구되면, 이웃 IDS 에이전트들은 광역 침입 탐지 행위에 협동적으로 참여하는 통합 침입 탐지와 대응 메커니즘을 제안하였다. Kachirski와 Guha (2003)은 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. Cai 등 (2006)은 패턴 인식에서 시작된 통계적 방법에 기초하여 모바일 애드 혹 망의 이동성 패턴과 같은 비정상 행위를 식별할 수 있는 비정상 탐지 알고리즘을 제시하였다. Bu 등 (2009)은 연속적인 경로 스트림에 대한 지역 클러스터를 구축하기 위하여 경로의 지역 연관성 특징을 이용하고, 가지치기 정책을 통하여 비정상 행위를 감시하는 이상적인 프레임워크를 제시하였다. Bae (2007)은 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 제안하였다. 그리고 이화주와 배인한 (2009)는 모바일 무선망에서 정상 이동 패턴으로 모바일 노드의 정상 프로파일을 구축하고, 이동 패턴 원소 간 비유사도 가중치 행렬을 이용하여 정상 프로파일로부터 어떤 모바일 노드의 이동 패턴의 비 유사도를 계산하여 비정상 행위 탐지하는 비유사도 기반 비정상 행위 탐지 방법을 제안하였다.

2.2. GPS 데이터

대부분의 GPS 수신기는 위성으로부터 반송파를 수신하여 현재 위치를 계산한 후에 데이터를 필요로 하는 다른 장치에 전송해야 한다. 전송할 때의 데이터 포맷이 제조 회사마다 다르다면 불편한 점이 많게 된다. 따라서 표준 데이터 포맷이 필요한데 현재 NMEA (National Marine Electronics Association)-0183이라는 포맷 방법이 사용되고 있다.

NMEA 문장은 주소 필드, 데이터 필드, checksum 필드로 구성되어 있다. 주소 필드는 Talker identifier와 Sentence formatter로 구성되고, Talker identifier는 데이터가 어디에서 오는지를 나타내는데,

GPS 수신기는 GP라는 두 문자를 사용하고 있다. Sentence formatter는 문장의 내용을 암시하는 식별자로 사용되는데, 항법에 유용하게 사용할 수 있는 식별자는 RMC와 GGA이다. NMEA 데이터는 프로그램에서 사용하기 쉽게 구성되어 있다. 일반적인 NMEA 데이터 형식은 다음과 같다.

$$\$< Address >,< Data >^*< checksum >< CR >< LF >$$

$<Address>로 표시된 주소필드는 <talker ID><sentence formatter>로 구분된다. 각 필드는 <Checksum>필드를 제외하고 콤마 (,)로 구분된다. 가장 유용한 NMEA 문장은 시간, GPS 상태, 현재위치, 속도, 진행방향, 날짜정보를 포함하고 있다.

표 2.1 실제 RMC 문장의 예

$GPRMC,083500.000,A,3551.9227,N,12843.7275,E,2.63,182.38,190910,,,A*60	
083500.00	Time of fix 08:35:00 UTC
A	Navigation receiver warning A=OK, V=warning
3551.9227,N	Latitude 35 deg. 51.9227 min North
12843.7275,E	Longitude 128 deg. 43.7275 min East
2.63	Speed over ground, Knots
182.38	Track Angle in degree true
190910	Date of fix 19 September 2010
,,	Magnetic variation
A	Mode indicator, (A=Autonomous, D=Differentia, E=Estimated, N=Data not valid)
*60	Mandatory checksum

표 2.1의 RMC 문장을 살펴보면, $GPRMC로 시작되는데, 이는 NEMA에 규정된 Talker ID (GP)와 Sentence formatter (RMC)이다. 이어서 UTC 시간정보가 오는데, 시분초로 구성된다. 다음에 오는 데이터 필드는 GPS 상태 지시자이며 A, V 등이 올 수 있다. 상태 지시자가 A일 경우 그 데이터는 유효한 것이고, V이면 유효성이 보장되지 않는다. 다음에 오는 2개의 데이터 필드는 위도 좌표와 North, South 지시자이다. 다음에 오는 2개의 데이터 필드는 경도 및 East, West 지시자이다. 그 뒤를 이어 속도 (Knots) 정보와 진행하는 방위각 정보, 날짜정보, 자기편차 정보가 따라온다 (Stefan, 2000).

2.3. 퍼지논리 이론

퍼지 집합은 일반적으로 크리스프 집합 개념을 확장한 것이다. 크리스프 집합론에서는 어떠한 원소가 집합에 속해 있는가, 속해 있지 않는가가 명료하게 나타난다. 그러나 퍼지집합에서는 원소가 그 집합에 속하는가, 아니면 속해 있지 않은가가 모호하게 표현되는 집합이다. Zadeh는 인간이 사용하는 언어의 의미, 개념 속에 포함되어 있는 모호성을 정량적으로 표현하는 방법으로 소속 함수를 사용하여 퍼지집합의 개념을 도입하였다. 일반적으로 전체집합 X에서 퍼지집합 A는 식 2.1로 정의된다.

$$\mu_A : X \rightarrow [0, 1] \tag{2.1}$$

여기서 μ_A는 퍼지집합 A의 특성을 나타내는 소속 함수라 하며, $x \in X$에 대한 소속 함수의 값 $\mu_A(X)$를 적합도라 하고, X가 퍼지집합 A에 속하는 정도를 폐구간 [0, 1] 사이의 임의의 값으로 나타낸다.

언어표현을 다루기 위하여 퍼지집합에서는 언어변수, 언어적 진리 값, 퍼지명제와 같은 것들이 정의되어 사용되고 있다. 언어변수란 자연언어의 단어를 변수 값으로 취급하는 것이다.퍼지제어 이론에서는 퍼지관계는 공정의 퍼지입력과 관련이 있고, 퍼지관계의 응용조건을 퍼지 제어규칙이라 한다. 예를 들

면 2개의 입력과 1개의 출력인 공정에 대하여 퍼지제어 규칙을 다음과 같이 정할 수 있다.

If E is PS and CE is PB, then CO is NE

If E is ZO and CE is ZO, then CO is ZO

여기서 E는 출력오차, CE는 오차변화량, CO는 출력변화량을 나타내고, 그리고 PE (Positive Big), PS (Positive Small), NM (Negative Meduim), ZO (Zero)는 퍼지변수를 나타낸다. 이와 같은 퍼지변수는 연속형과 이산형이 있다 (유종운, 1996; Zadeh, 1978).

3. FADA

최근에 GPS-폰과 GPS-PDA는 사람의 매일 생활에 널리 보급되고 있다. 그러한 장치로 사람들의 야외 이동성 추적과 위치 기반 응용 사용이 가능하게 하였다. GPS의 증가하는 인기로 GPS 데이터 기반 활동 인식은 과거 몇 년 동안에 상당한 주목을 받아왔다. 그러한 연구들은 개인의 중요한 장소 추출, 사람의 이동 예측, 사람의 교통 루틴 모델링을 포함한다 (Zheng 등, 2008).

GPS 로그는 일련의 GPS 포인트들 $p_i \in P$, $P = \{p_1, p_2, \ldots, p_n\}$이다. 각 GPS 포인트 p_i는 그림 3.1의 위도, 경도, 시간, 속도 등의 정보를 포함한다. 2차원 평면상에, 그러한 GPS 포인트들을 하나의 궤도로 순차적으로 연결할 수 있다. 그림 3.1은 GPS 로그로부터 특징을 어떻게 계산하는지를 보여준다. 2개의 연속 GPS 포인트 p_1과 p_2가 주어지면, 우리는 그것들 간의 거리 L_1, 시간 인터벌 T_1 그리고 방향 ($p_1.head$)을 계산할 수 있다. 방향의 기준은 북방이다.

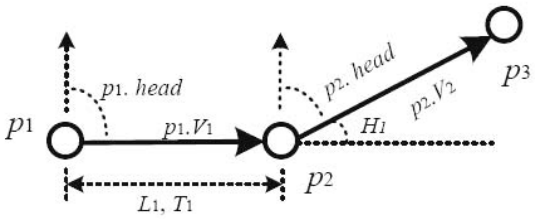

그림 3.1 GPS 로그에 기초한 특징 계산

따라서 p1의 속도는 식 3.1로 계산될 수 있다.

$$p_1.V_1 = L_1/T_1 \tag{3.1}$$

그리고 p1, p2, p3과 같은 연속 3 포인트의 방향 변경 $p_1.Dhead$는 식 3.2로 계산될 수 있다.

$$p_1.Dhead = |p_1.head - p_2.head| \tag{3.2}$$

우리는 GPS 로그로부터 3가지 특징: 위치 좌표 클러스터 (LCC, location coordinates cluster), 방향 변경률 (DCR, direction change rate), 속도 변경률 (VCR, velocity change rate)을 각각 추출한다.

모바일의 좌표를 이동 경로로 사용하기 위해서는 LCs의 입상을 감소시켜야 한다. 즉, 근접한 LCs는 하나의 클러스터로 변환한다. NMEA 명세에서 좌표정보는 ddmm.mmmm 형식으로 전달하도록 되어 있다. 여기서 dd는 경, 위도의 도 (degree)단위를 말하고 크기는 0∼360도로 나타낸다. mm은 분 (minute)을 말한다. 60분은 1도에 해당하며 .mmmm은 분의 소수점이하 수치로서 10진법이 적용된다.

mm.mmmm 부분을 60으로 나누어 산출되는 몫을 dd 부분과 더하면 dd.dddd 형식의 좌표를 구할 수 있다. LC의 원래 형식은 (###.####)과 (###,####)이다. 여기서 첫 번째 항과 두 번째 항은 위도와 경도를 각각 나타낸다. 농촌지역과 도심지역에 따라 다른 정확성 수준에 기초하여, 그 LC는 소수점 이후 구체적인 개수의 십진수로 절단되고 어림된다. 예를 들어, 수준 3으로, 첫 번째 항과 두 번째 항 (###.##)의 특정 십진수는 만일 그것이 0∼4내에 있으면 0으로 만일 그것이 5∼9 범위에 있으면 5로 어림된다. 즉, 예를 들어, LC 33.14623,114.26874는 33.10,114.25로 사상되어진다. 그림 3.2는 사용자 A의 이동 궤도상에 있는 일련의 GPS 포인트들의 LCs에 대한 LCCs의 예를 보여준다.

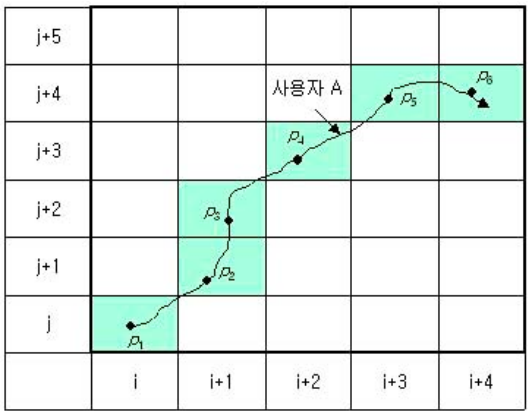

그림 3.2 사용자 A의 GPS 포인트들에 대한 LCs 클러스터의 예

다른 교통 방식의 방향은 트래픽 조건에 의존하지만 실제 루트에 의해 제한되므로 아주 다르다. 즉, 방향 변경률은 식 3.3으로 정의되어진다.

$$DCR = |P_c| / n \tag{3.3}$$

여기서 P_c는 사용자가 어떤 임계값 (H_γ)를 초과하여 이동 방향을 변경한 GPS 포인트들의 모임을 나타내고, $|P_c|$와 n은 P_c의 원소의 개수와 경로상의 GPS 포인트 개수를 각각 나타낸다.

이동 패턴을 분류하기 위하여 속도 변경률을 이용한다. 식 (3.4)를 사용하여 각 GPS 포인트의 $VRate$를 계산할 수 있다. 그리고 어떤 임계값 V_γ보다 큰 $VRate$를 갖는 GPS 포인트들의 개수를 얻을 수 있고, 식 (3.5)에 따라 VCR을 계산할 수 있다.

$$p_1.VRate = |V_2 - V_1| / V_1 \tag{3.4}$$

$$VCR = |P_v| / n \tag{3.5}$$

여기서 $P_v = \{p_i | p_i \in P, p_i.VRate > V_\gamma\}$이다. 따라서 VCR은 경로상의 전체 GPS 포인트들에서 어떤 임계값 이상 속도 변화를 갖는 GPS 포인트의 개수이다.

하나의 경로는 2개 이상의 패턴을 가질 수 있지만, 표 3.1은 6개의 GPS 포인트로 구성된 이동 경로의 하나의 이동 패턴에 대한 정상 프로파일의 예를 보여준다. 이러한 정상 프로파일 정보와 현재 이동 경로의 특징 정보를 사용하여 비정상 행위를 탐지한다.

표 3.1 모바일의 이동 경로에 대한 정상 프로파일의 예

경로	GPS 포인트	LCC	DCR	VCR
I	1	(34.10, 128.70)	0.4	0.4
	2	(34.10, 128.70)		
	3	(34.10, 128.75)		
	4	(34.10, 128.75)		
	5	(34.05, 128.80)		
	6	(34.05, 128.80)		

본 논문에서 제안하는 FADA의 전체적인 구조는 그림 3.3과 같다.

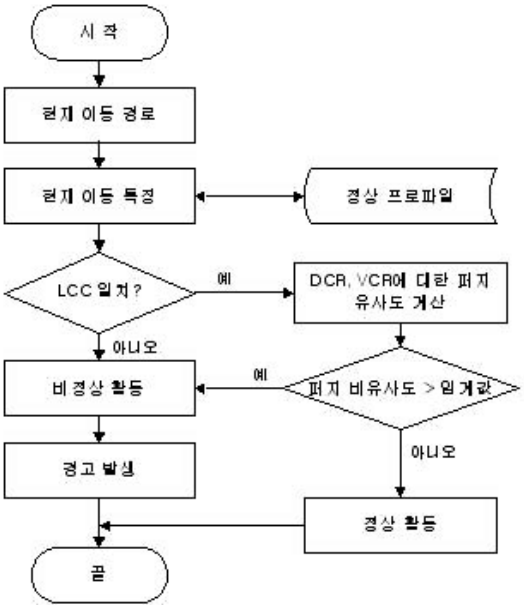

그림 3.3 FADA의 구조

먼저 정상 경로 및 특징 학습 알고리즘에서는 어떤 모바일 노드의 정상 이동 경로로부터 이동 특징을 추출하여, 그 노드의 정상 특징 프로파일을 구축한다. 그리고 비정상 행위 검사 알고리즘에서는 그 노드의 어떤 이동 활동이 발생하면, 그 경로가 정상 프로파일의 경로와 일치하는지 LCC들을 검사한다. 만일 일치하지 않으면 비정상 행위로 식별되어 경고가 발생하고, 아니면 정상 특징 프로파일로부터 그 이동 활동의 특징에 대한 DCR 퍼지 유사도와 VCR 퍼지 유사도를 그림 3.4, 그림 3.5와 같은 퍼지 소속 함수를 사용하여 각각 계산한다.

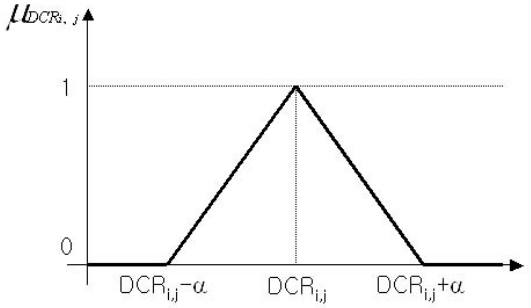

그림 3.4 $DCR_{i,j}$ 값에 대한 퍼지 소속 함수그림

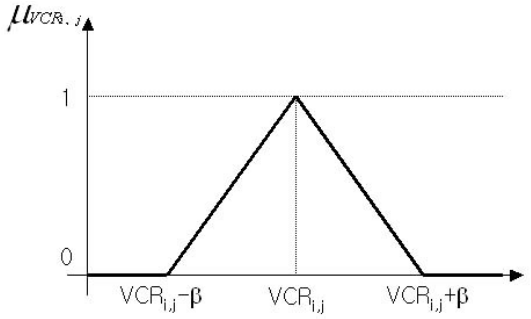

그림 3.5 $VCR_{i,j}$ 값에 대한 퍼지 소속 함수

여기서 $DCR_{i,j}$와 $VCR_{i,j}$는 i-번째 경로와 j-번째 패턴의 DCR 값과 VCR 값을 나타내고, 그리고 α와 β는 DCR 값과 VCR 값에서의 최대 허용 편차를 나타낸다. 퍼지 소속 함수를 사용하여 사용자 k의 현재 이동 경로 i에 대한 퍼지 비유사도는 식 3.6을 사용하여 계산될 수 있다.

$$\delta(k,i) = 1 - \ max_{j \in PF_{k,i}}(min(\mu_{DCR_{i,j}}, \mu_{VCR_{i,j}})) \tag{3.6}$$

여기서 $PF_{k,i}$는 사용자 k의 정상 경로 i에 대한 정상 패턴 프로파일 집합을 나타낸다. 따라서 $\delta(k,i)$는 사용자 k의 정상 경로 i의 정상 패턴 프로파일들 중에서 현재 이동 패턴과 가장 유사한 패턴을 갖는 이동 경로와 현재 이동 경로간의 퍼지 유사도를 먼저 구하고, 그리고 (1-퍼지 유사도)로 퍼지 비유사도를 구한다.

만일 계산된 $\delta(k,i)$값이 유사도 임계값인 Δ_{Sim}보다 크면 비정상 행위로 식별되어 경고를 발생시키고, 아니면 정상 이동 활동으로 식별되어진다.

4. 성능 평가

본 논문에서 제안하는 FADA의 성능을 평가하기 위하여 다음 2가지 척도를 사용한다.

- 탐지율: 비정상 행위로 측정된다. m'개의 비정상 행위에 대하여 n개가 비정상인 것으로 탐지되면, 탐지율은 n/m'으로 정의된다.

- 거짓 경고율: 정상 행위로 측정된다. m개의 정상 행위에 대하여 n개가 비정상인 것으로 식별되면, 거짓 경고율은 n/m으로 정의된다.

모의실험을 위하여 우리는 GPS 수신기를 사용하여 차량 이동 경로 그림 4.1와 보도 이동 경로 그림 4.2의 GPS 로그를 획득하고, 그 GPS 데이터를 분석하여 위치 클러스터의 스케일 된 좌표, 이동 변경률과 속도 변경률로 구성된 정상 이동 패턴의 프로파일을 구축한다. 그림 4.3과 그림 4.4는 2개의 경로에 대한 위치 좌표 클러스터에서의 정상 이동 패턴의 방향 변경 값과 속도 변경 값을 각각 보여준다. 여기서 이동 수단에 따라 다른 이동 패턴을 갖는다는 알 수 있다. 즉, 도보 이동 경로 II는 차량 이동 경로 I에 비해 위치 좌표 클러스터에서의 속도 변경 값은 작으나 반면에, 위치 좌표 클러스터에서의 방향 변경 값은 크다.

그림 4.1 경로 I (차량 이동)

그림 4.2 경로 II (도보 이동)

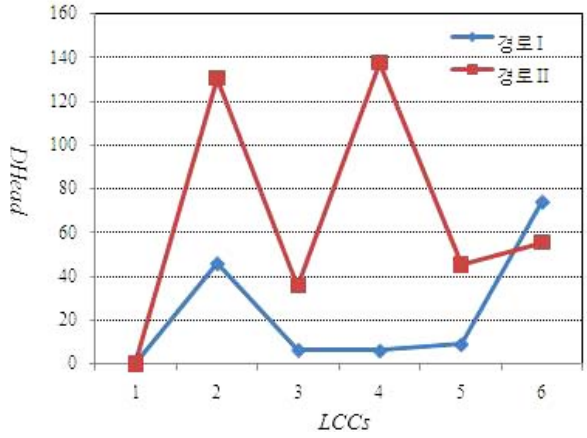

그림 4.3 위치 좌표 클러스터에서의 방향 변경 값

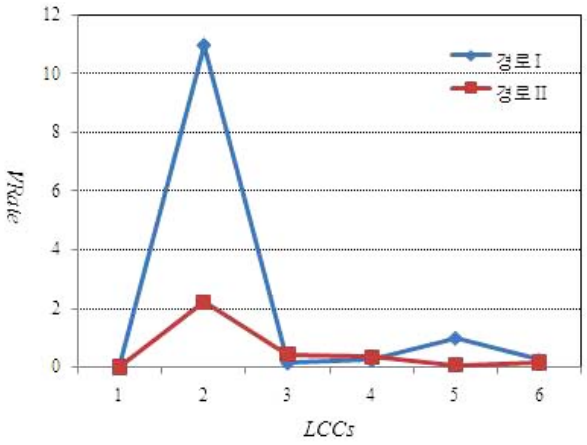

그림 4.4 위치 좌표 클러스터에서의 속도 변경 값

모의실험을 통하여 FADA의 성능을 분석하고 평가한다. 여기서 우리는 시뮬레이션 툴로 MATLAB 7.0 (Kay, 2009)를 사용한다. 표 4.1과 표 4.2는 모의실험에 사용한 시스템의 사양과 매개변수의 값을 각각 보여준다.

표 4.1 모의실험 시스템 환경

시스템	사양
GPS 수신기	FreeNavi GPS731
이동 단말기	Tablet PC SENS Q1b
시뮬레이션 툴	MATLAB 7.0
GPS 뷰어	locr GPS Photo

표 4.2 모의실험 매개변수와 값

매개변수	값
사용자 이동 횟수	100
정상 이동 경로의 개수	2
정상 이동 경로의 위치 좌표 클러스터의 개수	6
H_γ	45
V_γ	0.5
α, β	0.4
Δ_{Sim}	0.5

그림 4.5는 Baseline으로 62번의 정상 이동과 38번의 비정상 이동을 갖는 100번의 사용자 이동을 발생시킨 후, 사용자의 실제 이동 대 FADA의 예측 이동의 4가지 경우: N/N (Normal/Normal), N/A (Normal/Abnormal), A/N (Abnormal/Normal), A/A (Abnormal/Abnormal)의 발생 횟수를 보여준다. 본 논문에서 제안하는 FADA에서는 중요한 비정상 이동을 정상 이동으로 식별하는 A/N은 발생하지 않았으며, 정상 이동을 비정상 이동으로 식별하는 N/A가 1번 발생함을 알 수 있다.

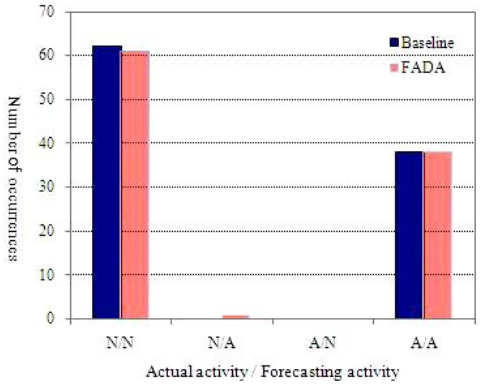

그림 4.5 사용자의 실제 이동 대 예측 이동의 발생 횟수

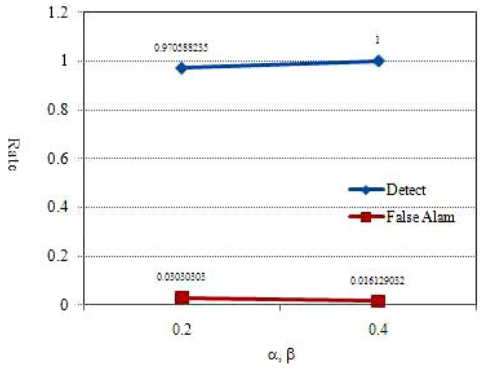

그림 4.6 DCR 값과 VCR 값의 최대 허용 편차에 따른 탐지율과 거짓 경고율

그림 4.6은 유사도 임계값이 0.5일 때, DCR 값과 VCR 값의 최대 허용 편차에 따른 퍼지 비정상 행위 탐지 알고리즘의 탐지율과 거짓 경고율을 보여준다. 본 모의실험 환경에서는 DCR 값과 VCR 값의 최대 허용 편차를 0.4로 설정하였을 때, 탐지율과 거짓 경고율에 대한 최적 성능을 제공함을 알 수 있다.

5. 결 론

최근에 이동 객체 추적 장치로부터 얻어진 추적 스트림에 대한 온라인 비정상 행위 감시에 대한 요구가 증가하고 있다. 제한된 공간 비용 내에서 고속 데이터 처리의 요구사항에 기인하여 이 문제는 흥미를 끌고 있다. 따라서 본 논문에는 모바일 애드 혹 망에서 모바일 장치의 GPS 로그로부터 이동 특징 정보를 계산하여 정상 프로파일을 구축하고, 모바일의 현재 이동 특징 정보와 프로파일내의 정상 이동 특징 정보간의 퍼지 비유사도를 계산한다. 그 계산된 퍼지 비유사도를 기초로 그 모바일 장치의 비정상 행위를 효율적으로 탐지하는 비정상 행위 탐지 알고리즘을 제안하고, 모의실험을 통하여 제안한 알고리즘의 성능을 평가하였다. 모의실험 결과, 제안하는 FADA의 정상 이동과 비정상 이동을 식별하는 N/N과 A/A의 발생 횟수가 사용자의 실제 이동인 Baseline과 거의 같다는 것을 확인하였다.

센서 데이터로부터 사람의 행위 인식과 사용자의 이동성 이해는 유비쿼터스 컴퓨팅 시스템에서 중요한 문제이다. 따라서 향후 연구 과제로는 스트리밍 추적으로 비정상 순서 패턴의 실시간 감시를 요구하는 많은 응용: 고령자 간호, 어린이 보호, 자동 운전 등에 관한 것이다.

참고문헌

이화주, 배인한 (2009). 이동 무선망을 위한 비유사도 기반 비정상 행위 탐지 방법의 설계 및 평가. <한국데이터정보학회>, **20**, 387-399.

유종운 (1996). 퍼지논리를 이용한 제어기술. <정보통신기술동향>, **11**, 45-59.

Bae, I. H. (2007). Design and evaluation of a dynamic anomaly detection Scheme considering the age of user profile. *Korean Data & Information Science Society*, **18**, 315-326.

Brutch, P. and Ko, C. (2003). Challenges in intrusion detection for wireless ad-hoc networks. *Proceedings of 2003 Symposium on Applications and the Internet Workshop*, 368-373.

Bu, Y., Chen, L., Fu, W. C. and Liu, D. (2009). Efficient anomaly monitoring over moving object trajectory streams. *KDD'09*, 159-167.

Cai, C., Guizani, S., Ci, S. and Al-Fuqaha, A. (2006). Constructing an efficient profile of ad-hoc node for mobility-pattern-based anomaly detection in MANET. *GLOBECOM*, 1-5.

Kachirski, O. and Guha, R. (2003). Effective intrusion detection using multiple sensors in wireless ad hoc networks. *HICSS'03*, 57-64.

Kay, M. G. (2009). *Basic concepts in matlab. Dept. of Industrial and System Engineering, North Carolina State University*, http://www.ise.ncsu.edu/kay/Basic_Concepts_in_Matlab.pdf.

Rezaul Karim, A. H. M., Rajatheva, R. M. A. P. and Ahmed, K. M. (2006). An efficient collaboration intrusion detection system for manet using bayesian approach. *MSWiM'06*, 187-190.

Stefan, J. (2000). Navigating with GPS. *Circuit Cellar*, **123**, 22-27.

Zadeh, L. A. (1978). Fuzzy sets as a basis for a theory of possibility. *Fuzzy Sets and Systems*, **1**, 3-28.

Zhang, Y. and Lee, W. (2000). Intrusion detection in wireless ad-hoc networks. *MobiCom'2000*, 275-283.

Zheng, Y., Li Q., Chen, Y., Xie, X. and Ma, W. Y. (2008). Understanding mobility based on GPS data. *UbiComp'08*, 312-3218.

Zhu, T. Q. and Xiong, P. (2005). Optimization of membership functions in anomaly detection based on fuzzy data mining. *Proceedings of the Fourth Int. Conf. on Machine Learning and Cybernetics*, 18-21.

Journal of the Korean Data & Information Science Society
2010, **21**(6), 1125–1136

한국데이터정보과학회지

FADA: A fuzzy anomaly detection algorithm for MANETs

Ihn Han Bae[1]

[1]School of Computer and Information Communication,
Catholic University of Daegu

Received 11 September 2010, revised 27 October 2010, accepted 1 November 2010

Abstract

Lately there exist increasing demands for online abnormality monitoring over trajectory stream, which are obtained from moving object tracking devices. This problem is challenging due to the requirement of high speed data processing within limited space cost. In this paper, we present a FADA (Fuzzy Anomaly Detection Algorithm) which constructs normal profile by computing mobility feature information from the GPS (Global Positioning System) logs of mobile devices in MANETs (Mobile Ad-hoc Networks), computes a fuzzy dissimilarity between the current mobility feature information of the mobile device and the mobility feature information in the normal profile, and detects effectively the anomaly behaviors of mobile devices on the basis of the computed fuzzy dissimilarity. The performance of proposed FADA is evaluated through simulation.

Keywords: Anomaly detection, fuzzy logic theory, GPS data, mobility pattern, similarity.

[1] School of Computer and Information Communication Engineering, Catholic University of Daegu, Gyeongbuk 712-702, Korea. E-mail: ihbae@cu.ac.kr.