

# 센서 네트워크 환경에서의 데이터 관리†

서강대학교 변창우\* · 박 석\*\*

버지니아대학교 손상혁

## 1. 서 론

최근 임베디드 시스템과 무선 통신 기술의 발전은 대규모적이면서 저비용적인 센서 네트워크 환경의 전개를 가능하게 하고 있다. 수천 개의 센서 노드들 간의 공동 작업을 기반으로 한 무선 센서 네트워크는 대규모 서식지 모니터링, 침입 탐지, 자동화된 실시간 위치 평가, 홈 어플리케이션, 과학적인 탐사 등 수많은 응용에 대한 새로운 플랫폼을 제공하고 있다.

이와 같은 센서 네트워크 환경의 데이터 관리는 두 가지 초점에서 살펴볼 수 있다. 첫 번째는 센서 데이터를 관리하는 부분이고, 두 번째는 센싱된 데이터에 의해 영향을 받는 데이터를 관리하는 부분이다.

센서 데이터를 관리하는 목적은 센서의 배터리 제약 사항과 무선 네트워크의 비 신뢰성을 극복하면서 센서 데이터의 정확성을 보장하는 것이다. 이에 대한 적합한 응용은 질의 처리 기술, 정보 수집과 유포에 대한 기술, 이벤트 서비스에 대한 기술 등이 있다.

무선 센서 네트워크에서의 질의 처리 기술은 통신비용을 절감하고 신뢰성을 향상시키는데 목적을 두고 있다. 또한 전통적인 데이터 집계 계산인 SUM, COUNT, AVG 그리고 MIN/MAX와 같은 간단한 유형의 데이터 집계 계산뿐만 아니라 복잡한 유형의 집계 계산을 지원해야 한다. [1,2]에서는 데이터 집계 계산을 위해 센서 노드로부터 데이터를 받아 기지국(base station)에서 최종 계산하는 방법을 탈피하여 네트워크 내부에서 데이터를 집계하고 최종 결과를 기지국에 보내는 방법에 대한 연구 및 영역에 대한 질의뿐만 아니라 중앙값 계산(median), 컨센서스 값과 같은 가장 빈도수가 높은 데이터 값, 분산된 데이터에 대한 히스토그램 등과 같이 질의 유형을 확장하고 이들에 대한 계산을 센서 네트워크 내부에서

계산하는 방법에 대한 연구를 진행하고 있다.

무선 센서 네트워크에서 필요한 데이터를 발견하는 방법은 센서 노드가 관찰된 데이터를 브로드캐스트하면 필요한 사용자가 그 정보를 받아보는 푸시(push) 방법과 사용자가 필요한 정보를 네트워크에 질의하면 그에 해당되는 정보를 갖고 있는 센서 노드가 정보를 전송하는 풀(pull) 방법이 있다. 전자는 네트워크에 그 정보를 필요로 하는 사용자가 많은 경우 효율적이지만, 정보에 대한 요구가 낮을 때 많은 브로드캐스트 대역폭이 낭비된다. 후자는 질의 빈도수가 관심 있는 이벤트의 빈도수보다 상대적으로 낮은 경우 필요한 경우만 통신을 하기 때문에 효율적이다. [3]에서는 언급한 두 가지 방법의 장점을 조합하여 질의 빈도수와 이벤트 빈도수에 따라 적절히 조절되는 효율적인 질의 처리 메커니즘인 "comb-needle" 질의 지원 모델에 대한 연구를 진행하고 있다.

이벤트 서비스[4]는 정확한 데이터 추출을 위한 신뢰 계산을 지원해야 하며, 실시간으로 작동하고, 에너지를 보존해야 한다. 또한 기본적으로 이벤트 서비스는 위치 및 이벤트 적용 범위를 인지하고 있어야 한다. 이벤트는 지역적으로 발생할 수 있고, 전역화 될 수 있으며 시스템의 많은 부분에서 동시에 발생할 수 있다.

센싱된 데이터에 의해 영향을 받는 데이터 관리 부분은 센싱된 데이터를 "상황 정보(context information)"라 하고 영향을 받는 데이터를 "자원" 혹은 "서비스"라 하여 상황-인식 기반의 보안[14,15]이라는 개념으로 소개되고 있다. 센서 네트워크 환경에서 상황-인식 기반의 보안의 목적은 센싱된 상황 정보를 기반으로 인가되지 않은 사용자가 공유된 정보에 불법적으로 접근하거나, 사용자 공유 정보를 노출 및 변경을 하지 못하도록 하는 것이다.

언급된 기술들 중에 본 고에서는 **센서 네트워크 환경에서의 이벤트 서비스에 대한 연구와 상황-인식 기반의 보안에 대한 최근 연구 현황을 소개한다.**

적절한 시간(right time), 적당한 장소(right place)에 정확한 센서 데이터가 수령자에게 도착해야 하는 실

† 본 연구는 정보통신부 정보통신연구진흥원에서 지원하고 있는 정보통신기초기술연구지원사업의 연구 결과의 일부임

\* 학생회원

\*\* 종신회원

시간과 정확성, 최적의 알고리즘을 기반으로 한 센서 노드의 배터리 소모를 줄이는 에너지 효율성, 센서 노드의 불규칙적인 패턴에 의해 생성된 센서 데이터에 대한 신뢰성 및 센싱 데이터에 의해 처리되는 응용의 안정성이 이에 해당된다.

2장에서는 이벤트 서비스와 상황-인식 기반의 보안에 대한 기존 연구에 대해서 간략히 소개하고, 3장에서는 정확한 데이터 추출을 위한 신뢰 계산을 지원하며, 실시간으로 작동하고, 에너지를 보존하면서 위치 및 이벤트 적용 범위를 인지하는 위치-인식 이벤트 서비스인 LAS(Location-aware Event Service)를 소개한다. 4장에서는 사용자 및 상황을 인식하고, 언제 어디서나 어떤 디바이스를 통해서도 끊이지 않는(Seamless) 서비스를 지원하는 상황 기반의 동적 접근제어 모델인 CBDAC(Content-based Dynamic Access Control) 모델을 소개한다. 마지막으로 5장에서는 결론과 함께 향후 연구 부분을 소개한다.

## 2. 관련 연구

센서 네트워크 상에서 데이터 서비스를 제공하는 연구가 많이 진행되고 있다. TinyDB 프로젝트는 애드 혹 센서 네트워크에서 정보를 추출하기 위한 질의 처리 기술을 연구하고 있다. 사용자는 SQL과 인터페이스를 통해 관심 있는 데이터를 기술한다. TinyDB는 내부-네트워크 집계 기술(in-network aggregation)을 이용하여 센서로부터 데이터를 수집할 수 있다[5, 6]. Cougar 프로젝트는 센서 네트워크를 분산 데이터베이스로 취급하여 센서 네트워크 상에서의 질의에 대해 연구하고 있다. 사용자의 질의가 들어오면 질의 최적기는 효율적인 질의 계획을 생성한다[7]. Narayanan et al.[8]은 센서 네트워크 상에서 정보를 얻기 위해 ACUQIRE 메커니즘을 제안하고 있다. 특정 질의에 대한 답을 찾기 위해 조정자 노드들은 부분적으로 질의를 해결하기 위해 어떤 홉 안에 모든 노드들로부터 정보를 집계한다. 일단 질의가 완전히 해결 되면 응답은 질의한 노드로 보내진다.

### 2.1 이벤트 서비스

센서 네트워크는 많은 분산 응용에 광범위하게 이용되고 있다. 여기서 위치 인식은 필수적인 시스템 특징 중 하나이다. 확장된 인프라 구조의 지원 없이 센서 노드로 하여금 자신의 위치를 발견하도록 하는 위치 파악에 대한 기술 연구가 진행되어 왔다.

Wood et al.[9]는 센서 네트워크 환경에서 혼잡한 위치를 감지하고 매핑하는 혼잡한 영역에서의 매핑 서비스(jammed-area mapping service)를 설계했다. 혼잡함이

감지되자마자 혼잡한 위치의 경계에 가까운 노드들은 혼잡한 위치 밖의 이웃들에 알려준다. 이런 노드들은 그룹을 형성하고 그룹들 간의 연합을 위해서 매핑 프로토콜을 이용하여 혼잡한 위치를 확대해 나간다. 그러나 센서 네트워크의 한 가지 유형의 센서만을 고려하고 있으며 프로그래밍 추상을 응용 개발자에게 제공하지 못하고 있다. 추가로 효율적인 방법으로 혼잡한 위치에 대한 재 표현 및 보고하는 방법을 해결하지 못하고 있다. Nowak and Mitra[10]는 반복적인 다이아터 부분 작업(recursive dyadic partitioning, RDP)을 이용하여 센서 네트워크에서 경계 측정을 위한 방법을 제안했다. 이론적으로 그들의 알고리즘이 경계의 평방-제곱 에러(mean-square error)와 에너지 소비 사이의 최적의 상쇄현상을 보여주고 있다. Hellerstein et al.[11]은 TAG 기반의 공간상에서 센서 값 분포에 대해 지도를 작성하는 등고선 매핑을 제안하고 있으며, Bakshi et al.[12]는 센서 네트워크 상에서 관심 있는 위치의 레이블링과 신원파악의 기본 문제에 대한 알고리즘을 제안하고 있다. Devaguptapu et al.[13]는 센서 네트워크 상에서 두 개의 특별한 문제점을 풀고자 이미지 처리 기술을 적용하여 상호 관련 없는 센서 노이즈를 청소하는 것과 분산화된 가장 자리를 감지하는 기술을 제안하고 있다. 시뮬레이션 결과 성능은 센서의 밀집 상태에 상당히 의존하고 있음을 보여주고 있다. 위의 모든 기술들은 센서 관독에 대한 간단한 기능 또는 단일 노드의 상태 따라 어떤 이벤트를 감지하는 상호관련된 정보 처리에 대한 요구를 충분히 소화하고 있지 않다.

### 2.2 상황-인식 기반의 보안

기존의 역할 기반 접근제어(Role-Based Access Control : RBAC)[16]는 접근 결정이 개개인의 사용자들이 조직원으로서 요구되는 역할에 근거하여 이루어진다. 접근 권한은 역할 이름에 따라 그룹화 되고, 이러한 역할이 개개인의 업무적 책임과 권한에 따라 사용자에게 부여됨으로써 자원의 이용이 제약된다. 그러나 기존 역할 기반 접근제어 모델로는 상황에 따른 접근제어를 수행할 수 없다. 보안의 강화와 사용자의 상황에 따른 유연한 정보 접근을 위하여 상황 정보를 접근제어에 이용하는 연구가 진행되고 있다.

xoRBAC 모델[17]은 상황 정보를 접근제어 결정에 이용하기 위하여 역할 기반 접근제어의 제약사항을 이용한다. 상황 제약사항(context constraint)은 상황 속성의 실제 값을 미리 정의된 조건 값과 비교하여 접근을 통제한다. 이는 매우 정적이다.

GRBAC(Generalized Role-Based Access Control :

GRBAC) 모델[18,19]은 접근제어 결정에 사용자 역할 (subject role), 객체 역할(object role), 환경 역할 (environment role)을 사용함으로써 기존 역할기반 접근제어를 확장하였다. 사용자, 객체, 환경 요소를 역할 계층으로 구조화함으로써 접근제어 정책 기술의 단순함과 융통성을 제공한다. GRBAC 모델은 시간이나 위치와 같은 환경 요소를 환경 역할로 정의하여 접근제어 정책에 기술한다.

그러나 xORBAC과 GRBAC 모델은 상황정보에 대한 범용적이고 일반적인 정의를 사용하지 않고 있다. 또한, 계층 구조의 이용에 따른 진과 규칙 때문에 발생하는 충돌 문제 및 상황을 구성하는데 생기는 의미적 충돌 문제를 고려하고 있지 않다.

### 3. 위치-인식 이벤트 서비스(Location-Aware Event Service: LAS)

LAS는 이벤트 발생을 감지하여 통보하고, 사용자에게 이벤트의 유효 적용 범위의 정확한 측정을 제공하는 것을 목표로 하고 있다.

이번 절은 이벤트 서비스의 기반이 되는 이벤트를 분류하고 LAS에 대한 개요 및 필요한 가정들을 소개하고 나서 LAS의 각 컴포넌트를 설명한다.

#### 3.1 이벤트 분류

센서 네트워크에서의 이벤트 서비스는 사용자로 하여금 센서 네트워크에서 생성된 대용량의 데이터에서 원하는 정보를 추출하고 효율적인 방법으로 그 환경을 주시하도록 도와준다. 모든 가능한 관심 있는 이벤트를 나열하기 보다는 센서 네트워크에서 특히 중요한 다섯 가지 특성들을 기준으로 분류한다. 표 1은 분류된 이벤트를 보여준다.

첫 번째 차원은 적용 범위이다. 포인트 이벤트는 적용 범위가 단일 포인트와 같은 매우 작은 범위의 이벤트를 말한다. 영역 이벤트는 어떤 영역 범위에 둘러싸인 이벤트를 말한다. 영역이 크면 많은 노드들 사이의 공동 작업이 필요하고 불규칙하기 때문에 이벤트의 신뢰성을 위해 영역 이벤트의 윤곽을 재 표현하는 것도 중요하다.

두 번째 차원은 위치이다. 정적 위치 이벤트는 이벤트 기간 동안 위치가 고정된 이벤트를 말하는 반면 동적 위치 이벤트는 이동 가능하다. 동적 위치 이벤트를 위해서 이벤트 서비스는 이벤트를 계속 추적해야 하고, 이벤트의 현재 적용 범위와 움직인 방향 및 속도 등과 같은 많은 정보가 지원되어야 한다.

손실은 세 번째 차원이다. 파괴적 이벤트는 이벤트 기간 동안 노드들이 파괴되어 임무를 실패할 수 있는 이벤

표 1 이벤트 분류

이벤트 (Events)	적용 범위 (Coverage Area)	포인트 이벤트 (Point Event)
		영역 이벤트 (Area Event)
	위치 (Location)	정적 위치 이벤트 (Static Location Event)
		동적 위치 이벤트 (Dynamic Location Event)
	손실 (Damage)	파괴적 이벤트 (Destructive Event)
		비파괴적 이벤트 (Non-destructive Event)
	지속성 (Duration)	단기 이벤트 (Short-lived Event)
		장기 이벤트 (Long-lived Event)
	합성 (Composition)	원자적 이벤트 (Atomic Event)
		혼합 이벤트 (Compound Event)

트를 말한다. 따라서 센서 노드로부터 “무의미 데이터 (blank data)”가 발생할 수 있다.

네 번째 차원은 이벤트의 동작 기간이다. 장기 이벤트의 중요 이슈는 어떻게 사용자가 이벤트를 계속 추적할 수 있도록 이벤트가 보고 되는가이다. 다시 말하면, 보고 되는 이벤트의 신선함과 에너지 소비 사이에 충돌이 발생한다.

마지막 차원은 합성이다. 원자적 이벤트는 단일 센서에 의한 낮은 단계의 이벤트이다. 반면 혼합 이벤트는 다수의 센서 데이터 사이의 상호 관계를 요구하는 이벤트이다.

#### 3.2 서비스 구조

LAS는 사용자와 물리적 환경 사이의 가교 역할을 한다. 무선 네트워크에서 사용자는 네트워크와 직접적인 통신 없이 무선 네트워크 상에서 관심 있는 이벤트를 감지할 수 있다.

그림 1처럼 LAS는 전송 계층 위의 응용 계층에 위치한다. 사용자 인터페이스(API)에서는 사용자가 관심 있는 이벤트를 등록하고 삭제하는 기능이 제공된다. 이벤트 감지 서비스는 시간 윈도우 메커니즘, 위치 측정 모듈, 그리고 최종 보고 생성 모듈 이렇게 세 개의 핵심 컴포넌트들로 구성된다. 시간 윈도우 메커니즘은 시간적으로 상호관계를 맺은 센서의 원자적 이벤트 보고를 수집하는 방법을 제공한다. 이름에서 알 수 있듯이 위치 측정 모듈은 위치와 이벤트 적용 범위를 감지한다. 이것은 원자적 영역 합집합 알고리즘(atomic area union algorithm)과 원자적 이벤트들 간의 교집합 알고리즘(intersection across atomic events algorithm)으

로 구성되며 원자적 이벤트의 적용 범위와 혼합 이벤트의 적용 범위를 감지하는 책임이 있다. 최종 보고 생성 모듈은 최종 이벤트 보고를 생성하고 사용자가 기술한 이벤트를 보고하는 방법을 결정한다.

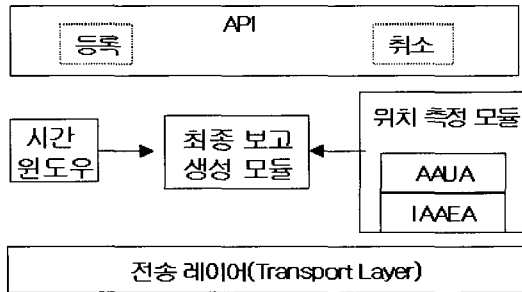


그림 1 서비스 구조

### 3.2.1 가정

LAS설계에 있어서 필요한 가정은 다음과 같다.

- 노드가 자신의 위치를 알 수 있는 위치 서비스가 지원된다.
- 시스템 초기화 시, 네트워크는 정적으로 어떤 위치를 기반으로 고정된 크기의 그룹들로 나뉜다. 그룹 리더 노드는 다른 노드에 비해 높은 메모리 능력과 처리 능력을 갖고 있다. 초기화 동안 각 노드는 자신의 위치를 기반으로 어떤 그룹에 속하게 된다.
- 이벤트의 적용범위는 사각형으로 간주한다. 일단 이벤트가 발생하면 영향을 받은 영역 안에는 충분한 센서 노드들이 존재한다. 만약 센서 네트워크가 균등하게 전개되어 있다면 감지 가능한 이벤트의 최소 크기에 대한 정확한 요구사항을 주기는 어렵다. 그러므로 감지 가능한 영역 이벤트 크기 S는 다음의 요구사항을 만족해야한다.

$$S = \frac{\text{width of the area event's coverage area}}{\text{AVGD}} > 1$$

$$\text{AVGD} = \sqrt{\frac{\text{NetworkArea}}{\text{The number of nodes}}}$$

### 3.2.2 이벤트 등록 및 취소 인터페이스

이 인터페이스를 통해 사용자는 관심 있는 이벤트를 쉽게 등록하고 이미 등록된 이벤트의 감지를 취소할 수 있다. 본 고에서는 이벤트 등록 및 취소 기능을 표현하는 자체 언어를 개발하기 보단 다음과 같은 SQL과 유사한 문장을 이용한다.

```
INSERT INTO EVENT_LIST
(EVENT_ID, DETECTING_AREA, SUBEVENT_SET,
REGISTRANT_SET, DETECTION_DURATION
[, TEMPORAL_RESOLUTION])
```

```
(, DISCRIMINATING_DISTANCE)
[, REPORT_OPTIONS]
[, ACTIONS])
```

위 문장의 목적은 DETECTING\_AREA 안에 있는 노드들에게 DETECTION\_DURATION 동안 EVENT\_ID의 특정 이벤트를 감지하도록 요청하는 것이다. 일단 이벤트가 감지되면 REGISTRANT\_SET 안에 있는 모든 노드들에게 보고 된다. TEMPORAL\_RESOLUTION은 다른 이벤트라고 간주될 수 있는 시간 차원에 의한 감지 단위를 기술한다. REPORT\_OPTIONS은 이벤트를 보고하는 방법을 기술한다. DISCRIMINATING\_DISTANCE는 두 개의 원자적 이벤트를 구별하는 방법을 제공한다. 그리고 ACTIONS은 이벤트 발생과 관련된 행위들을 기술한다. 추가로 SUBEVENT\_SET은 시간 윈도우의 크기, 혼합 이벤트를 구성하고 있는 하부 이벤트 집합, 신뢰 함수 그리고 관련된 혼합 이벤트의 발생을 결정하는데 필요한 최소 신뢰 값을 기술한다.

등록된 이벤트는 DETECTION\_DURATION이 종료되기 전이라도 다음과 같은 삭제 요구를 보냄으로써 삭제될 수 있다.

```
DELETE FROM EVENT_LIST
WHERE EVENT_ID = event_id
```

### 3.2.3 시간 윈도우

원자적 이벤트를 감지하자마자(즉, 임계 값보다 센서가 판독한 값이 큰 경우에 해당된다), 노드는 즉시 그룹 리더에게 타임스탬프된 원자적 이벤트 발생을 통보한다. 여기서 그룹 리더가 원자적 이벤트 발생 통보를 기다리는데 필요한 시간은 중요한 요소이다. 시간 윈도우의 크기를 선택하는 것은 관심 있는 이벤트의 의미에 종속된다. 만약 시간 윈도우가 매우 작다면 그룹 리더는 정확한 의사결정을 하는데 충분한 정보를 수집할 수 없다. 그렇다고 시간 윈도우가 너무 커버리면 수집한 이벤트 통보는 실제 다른 이벤트를 참조할 수 있고, 구식이 되어 버릴 수 있다. 이벤트가 리더에게 보고될 때 슬라이딩 시간 윈도우가 생성된다. 같은 영역에서 발생된 다수의 동시적인 혼합 이벤트가 존재할 수 있다. 그때는 그룹 리더는 각각 다른 이벤트들에 대해 하나의 시간 윈도우를 시작한다.

### 3.2.4 위치 측정 모듈

위치 측정 모듈은 위치-인식 이벤트 서비스의 핵심 역할을 담당한다. 그룹 리더에 의해 수집된 원자적 보고들을 기반으로 위치 측정 모듈은 이벤트의 적용 범위를 계산한다. 간단히 말해서, 만약 영역 이벤트가 과수원의 건조 위치를 감지하는 하나의 원자적 영역 이벤트이라

면, 그룹 리더는 이벤트의 위치와 원자적 이벤트를 보고한 모든 센서의 적용 범위를 합한 적용 범위를 측정하기 위해 AAUA를 이용한다. 그러나 만약 관심 있는 이벤트가 다수의 하부 이벤트들로 구성된 혼합 이벤트라면 그룹 리더는 두 단계를 진행할 필요가 있다. 첫째, 각 하부 이벤트의 적용 범위를 AAUA를 이용하여 측정한다. 그런 후 동시에 모든 하부 이벤트가 존재하는 적용 범위를 결정하기 위해 IAAEA를 통해 영역에 대한 교집합을 계산한다.

가. 원자적 영역 합집합 알고리즘(Atomic Area Union Algorithm: AAUA)

원자적 이벤트의 적용 범위를 측정하는 것은 보기보다 어렵다. 센서가 보낸 원자적 이벤트 보고들이 있다면 어떻게 시간적으로 상호 관련되게 보고들을 조합해야 하는가? 어떻게 정확하게 적용 범위의 경계를 계산할 수 있을까?

이와 같은 질문을 고려하여 원자적 영역 합집합 알고리즘은 다음과 같이 작동한다:

단계 1: 분류화

정의된 이벤트의 시간적 의미를 이용하여 그룹 리더는 시간적으로 상호 관련된 원자적 이벤트 보고를 수집한다. 혼합 이벤트의 발생은 다수의 원자적 이벤트들로 구성될 수 있기 때문에 그룹 리더는 처음에 원자적 이벤트 유형에 따라 수집된 원자적 이벤트 보고를 분류해야 한다.

단계2: 폭넓은 적용 범위 측정(Coarse Coverage Estimation)

이 단계의 목표는 각 원자적 이벤트의 적용 범위를 폭넓게 측정하는 것이다. 같은 유형의 두 개의 센서에 의해 감지된 영역을 합칠 수 있을 것인가에 대한 결정을 위해 기준으로 “차별 거리 (discriminating distance)”라는 개념을 도입한다. 만약 두 개의 센서 A와 B의 위치적인 거리가 사용자에게 의한 이벤트의 의미적인 부분으로 기술된 “차별 거리”라는 임계 값보다 작다면 같은 유형의 원자적 이벤트를 감지하도록 한다.

단계 3: 실제 적용 범위 측정(Fine Coverage Estimation)

첫 번째 단계와 두 번째 단계를 통해 공간적으로 상호 관련된 센서들에 의해 감지된 영역을 합침으로써 원자적 이벤트의 적용 범위가 폭 넓게 계산된다. 그러나 측정된 적용 범위는 실제 적용 범위라 할 수 없다. 그림 2는 위에서 언급한 폭 넓은(coarse estimation) 측정에 의해 발생된 “경계 효과”라 불리는 문제점을 보이고 있다. 내부 사각형은 실제 적용 범위를 표시하고 외부 사각형은 폭 넓은 측정에 의한 결과이다. 그리고 원은 같은 유형의 센

서들로부터 센싱된 적용 범위를 표현한다. 실제 적용 범위 밖의 센서들은 원자적 이벤트를 감지할 수 있기 때문에 폭넓게 측정된 영역은 실제 영역보다 넓다. 분명 센싱 영역 R이 넓으면 넓을수록 “경계 효과”는 더욱더 심하다.

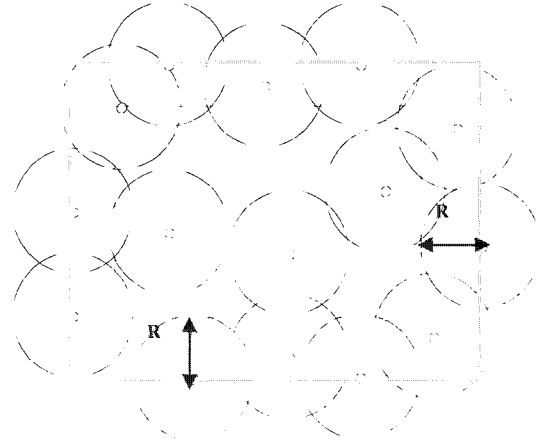


그림 2 경계 효과

경계 효과를 처리하기 위해 폭넓게 측정된 영역을 그림 3처럼 작고 바람직한 측정을 얻기 위해 줄일 필요가 있다. 여기서 D는 조정 거리를 의미한다.

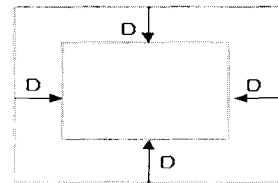


그림 3 작고 바람직한 측정

D는 네트워크 밀집상태, 이벤트 크기 그리고 센서의 센싱 영역을 고려하여 계산된다. D에 따라 폭넓게 측정된 영역을 조정함으로써 보다 정확한 이벤트 적용 범위 측정치를 얻을 수 있다. D를 위한 보다 높은 성능을 내는 계산 모델을 찾는 연구가 진행되고 있다.

나. 원자적 이벤트들 간의 교집합 알고리즘(Inter-section Across Atomic Events Algorithm: IAAEA)

위에서 제시한 원자적 영역 합집합 알고리즘은 원자적 이벤트에 대한 적용 범위만을 처리한다. 네트워크 상의 어떤 곳에서 다수의 하부 이벤트들로 구성된 혼합 이벤트가 발생한다고 가정하자. 처음에 그룹 리더는 각각의 하부 이벤트의 적용 범위를 결정하기 위해 원자적 영역 합집합 알고리즘(AAU)을 이용해야 한다. 그 다음 혼합 이벤트의 존재성을 판단하기 위해 신뢰 함수와 그 혼합 이벤트의 적용 범위를 측정하기 위해 원자적 이벤트들 간의 교집합 알고리즘에 의존한다.

혼합 이벤트의 발생은 다수의 상호 관련된 하부 이벤

트들로 구성된다. 예를 들어, 높은 온도, 강렬한 빛 그리고 굉음은 세 개의 원자적 이벤트들로 이들에 의해서 폭발이 일어났음을 암시할 수 있다. 신뢰 함수는 혼합 이벤트를 구성하는 하부 이벤트들 간의 관련 정도를 기술한다. 신뢰 함수는 간단히 선형 방정식 혹은 복잡한 통계 모델이 될 수 있다[8]. 만약 신뢰 함수의 결과인 신뢰 값이 사용자가 기술한 최소 신뢰 값보다 큰 경우 혼합 이벤트가 감지되었다고 볼 수 있다.

### 3.3 최종 보고 생성 모듈

시간 윈도우와 위치 측정 모듈을 이용하여 그룹 리더는 정확하게 시간적으로 상호 관련된 센서의 원자적 보고를 기반으로 이벤트 적용 범위를 측정할 수 있다. 시스템의 또 다른 중요한 컴포넌트는 최종 보고 생성 모듈이다. 이것은 센서 네트워크 상에 감지된 이벤트를 통보하는 방법을 결정한다.

그룹 리더는 감지되었던 모든 영역 이벤트를 기록한다. 어떤 영역 이벤트에 대한 엔트리는 DETECTION DURATION이 종료되거나 사용자가 명시적으로 등록된 이벤트 감지를 삭제할 때까지 삭제되지 않는다.

## 4. 상황기반의 동적 접근제어(Context-Based Dynamic Access Control: CBDAC)

전통적인 조직 내의 컴퓨팅 환경에서 구성원들이 조직 내의 자원들을 접근하기 위해서는 적절한 접근정책의 적용을 받아야 한다. 주요 접근제어 방법으로는 강제적 접근제어, 임의적 접근제어, 역할기반 접근제어 등의 접근제어 모델들이 제시되었다. 이들 모델의 핵심 요소는 주체, 객체 그리고 추가로 역할 등이다. 그러나 실제 작업 환경 속에 컴퓨터가 조용하게 스며들어 우리에게 필요한 정보를 제공하고, 처리하며, 여러 가지 서비스를 수행하면서 도와주는 센서 네트워크 기반의 응용에서는 스며든 컴퓨터들로부터 센싱된 상황 정보를 이용하여 미리 시스템에 정의된 접근 정책에 수집된 상황 정보를 조합한 동적인 접근제어 모델이 필요하게 되었다. 특히, 핵심 요소인 주체, 역할, 서비스 그리고 객체에 새로운 추가 정보가 필요하다. 그림 4는 동적 접근제어 모델의 핵심 요소들 간의 관계를 보여주고 있다.

- **주체** : 동적인 접근제어 모델 주체에 대한 신원 확인은 실제 사용자가 직접 입력하여 확인되는 경우도 있고, 혹은 센서들에 의해 사용자의 신원이 확인된다. 여기서 관리되어야 하는 상황 정보로는 사용자의 위치, 접근 시간 등이다.
- **역할** : 기존 역할기반 접근제어 모델에서의 역할은 조직체의 구조를 반영한 역할 계층을 임무분리와

같은 제약사항으로 역할 관리를 수행하였다. 그러나 센서 네트워크 환경에서는 다양한 제약사항이 존재한다. 시간 상황 정보를 지원 받는 역할 구동 시간, 위치 상황 정보를 지원 받는 역할 접근 위치, 역할이 작동되는 공간적인 영역 등의 역할 고유의 추가 정보가 필요하다. 그리고 주체 인증을 지원하는 접근 허용된 주체와의 관계 정보가 필요하다.

- **서비스** : 기존 역할 기반 접근제어 모델에서 권한에 해당되는 부분이다. 서비스 자신의 구동 시간, 서비스 자신의 구동 영역이 추가 정보로 필요하다. 추가로 원자적인 서비스가 있는 반면, 여러 원자적 서비스들이 조합된 혼합 서비스도 존재한다. 따라서 서비스 관리의 편리성을 위하여 서비스에 구조를 적용하는 것도 고려할 사항이다.
- **객체** : 객체 구동 시간과 같은 객체 자신의 고유 정보가 추가로 필요하며, 명시적으로 또는 묵시적으로 서비스와의 관계 정보도 접근 정책에 반영되어야 한다. 추가로 객체 관리의 편리성을 위하여 객체에 구조를 적용하는 것도 고려할 사항이다.
- **역할-서비스-객체** : 역할이 객체를 할당 받은 서비스에 할당되었을 때 이 관계의 유지 시간과 구동 영역에 대한 추가 정보가 필요하다.
- **부분 역할, 부분 서비스, 부분 객체** : 센싱된 주체에 대한 정보는 센싱 환경(무선 네트워크 환경, 노이즈 센서, 센서 정보의 일부 손실 등)에 의해 그 정확도가 100%가 아닐 경우도 발생한다. 그런데 100% 정확하지 않다고 해서 무조건적인 접근 불허 정책은 때론 바람직하지 않다. 따라서 같은 역할이라도 정확도에 따라 부분 역할을 할당하여 어느 정도의 기본 서비스를 받을 수 있는 부분 서비스, 기본 서비스를 위한 부분 객체의 개념이 필요하다. 본 고에서는 아직 이 부분에 대해서 다루지 못하고 있으며 향후 연구 계획을 갖고 있다.

## 4.1 상황 정의

### 4.1.1 기본 상황 정의

시간, 위치와 같이 상황을 구분하는 기준으로 상황 정보들이 갖는 속성을 차원이라 하고, 각 차원을 구성하는 상황 정보로 원자 값을 갖는 상황 정보와 원자 값을 갖는 상황 정보를 그룹으로 묶는 상황 정보를 "기본 상황"이라고 정의한다. 예를 들면, 시간 차원에 속하는 시간, 날짜, 요일 등의 상황 정보는 시간 기본 상황에 포함될 수 있고, 위치 차원에는 센서가 포함된 사용자가 위치할 수 있는 위치 정보가 위치 기본 상황으로 포함될 수 있다. 각 차원에 속하는 기본 상황은 상황 정보의 포함관계

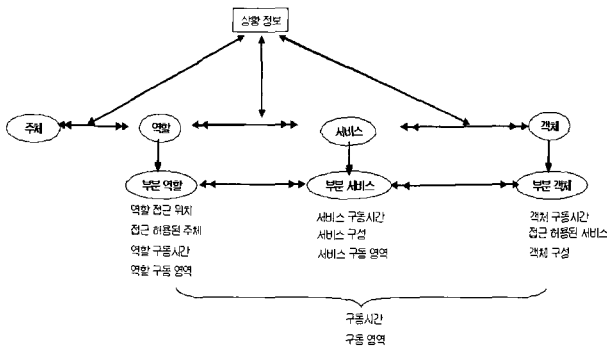


그림 4 동적 접근제어 모델의 요구사항

에 따라 상황 계층구조를 구성할 수 있다. 상황 계층구조의 하위에 존재하는 상황은 상위에 존재하는 상황에 비해 상세하다. 따라서 상황의 발생의 전과 방향은 하위에서 상위로 향하고 특정 하위 상황의 발생은 상황 계층 구조상에서 그 상황의 상위 상황의 발생을 일으킨다.

#### 4.1.2 사용자 정의 상황(User-defined Context) 정의

사용자 정의 상황은 시스템 관리자나 사용자가 원하는 상황에 정보의 접근을 허용하거나 거부하는 것을 기술하는데 사용되는 상황 정보이다. 하나의 기본 상황과 조건을 속성으로 갖는 상황 정보를 단일 상황(single context)이라 정의하고 두 개 이상의 단일 상황으로 구성된 상황 정보를 복합 상황(compound context)이라고 정의한다. 복합 상황은 구성 요소의 결합에 따라 AND 상황과 OR 상황으로 구분된다. 상황 정보들이 or-관계로 결합된 복합 상황을 OR 상황(OR context)이라고 정의한다. OR 상황은 구성 상황 정보들 중 적어도 하나가 참일 때, 참 값을 갖는다. 즉, 상황 구성 상황 정보들 중 적어도 하나만 활성화 되면 OR 상황도 활성화됨을 의미한다. 상황 정보들이 and-관계로 결합된 복합 상황을 AND 상황(AND context)이라고 정의한다. AND 상황은 구성 상황 정보들이 모두 참일 때 참 값을 갖는다. 즉, 상황 구성 상황 정보들이 모두 활성화 되었을 때 AND 상황도 활성화됨을 의미한다.

### 4.2 정책 기술

기본 상황 및 사용자 정의 상황을 고려한 권한부여 규칙은 다음과 같은 형식으로 표현된다.

< Subject, Role, Service, Object, [Context1 [con Context2 [con ...]], sign>

단, con = { & or | }, sign = { + (허용) or - (거부) }

[Context1 [con Context2 [con ...]]은 상황이 없거나 하나 이상의 상황을 나타낸다. con은 연결 유형(conjunction type)으로 and-결합을 의미하는 & 유형과 or-결합을 의미하는 | 유형이 있다. and-결합으로

연결된 상황은 연결된 모든 상황이 참 값을 가질 때, 즉 모두 활성화 되었을 때 권한부여 규칙이 적용됨을 의미한다. 반대로, or-결합으로 연결된 상황은 연결된 상황 중 적어도 하나의 상황이 활성화 되었을 때 권한부여 규칙이 적용된다.

### 4.3 상황을 이용한 접근제어 수행 과정

사용자의 접근 요청에 대하여 권한을 부여하기 위하여 사용자의 역할, 객체와 함께 상황 정보를 고려하여 권한평가를 수행한다. 사용자가 특정 역할을 갖고 특정 서비스를 수행하고자 한다면 시스템에는 사용자의 상황(접근 시간, 위치 등)도 함께 전달된다. 일단 인증 실행기(Authentication Executor)에 의해 사용자가 주어진 상황 정보를 기반으로 그 상황에서 시스템의 주체로서 자격이 있음을 인증한다. 인증된 사용자에게는 주체-역할 관리기(Subject-Role Manager)에 의해 해당되는 역할이 활성화된다. 사용자의 상황 정보를 계승한 역할 상황 정보를 기반으로 선택한 역할이 활성화될 수 있음을 확인한다. 활성화된 역할에는 역할-서비스 관리기(Role-Service Manager)에 의해 해당되는 서비스가 활성화된다. 이때 서비스-객체 관리기(Service-Object Manager)에 의해 해당되는 객체 역시 활성화된다. 역할 상황 정보를 계승한 서비스 상황 정보(위치, 시간 등)를 기반으로 선택한 서비스가 활성화 될 수 있는지의 여부를 접근권한 실행기에서 판단한다. 그림 5는 사용자의 접근 요청에 대한 접근제어 수행 과정을 나타낸다.

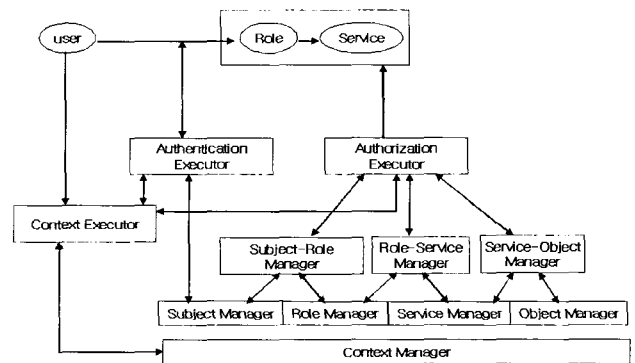


그림 5 접근제어 수행 과정

#### 4.3.1 권한부여 규칙 탐색

역할-서비스-객체 계층 구조를 기반으로 한 허용권한과 거부권한의 권한 전과 규칙은 그 각각을 고려해야 하기에 복잡하다. 허용권한은 계층 구조의 하위에서 상위로 권한이 전파되므로 계층 구조에서 하위에 존재하는 것들이 가지는 권한이 같이 평가되어야 한다. 거부권한은 허용권한과 반대 방향으로 권한이 전파되므로 계층 구조에서 보다 상위에 존재하는 것들이 가지는 권한도

평가되어야 한다. 예를 들어, 역할-서비스-객체 관계에서 임의의 어느 서비스의 거부권한 여부를 판단하기 위해서는 그 서비스의 상위에 존재하는 서비스를 찾고, 추가로 그 서비스와 관련된 역할에서의 상위 역할, 객체에서의 상위 객체를 찾는다. 허용권한을 평가하기 위하여 그 서비스의 반대 방향으로 권한을 찾으면 된다.

#### 4.3.2 권한부여 알고리즘

찾은 권한 규칙들에서 권한 부여를 위하여 허용권한과 거부권한이 기술된 권한부여 규칙에 대하여 비교를 수행한다. 먼저, 거부 권한이 기술된 권한부여 규칙이 존재한다면 허용권한이 기술된 권한부여 규칙이 존재하는지 비교한다. 만약, 허용권한이 기술된 권한규칙이 존재한다면 권한 충돌이 발생하므로 충돌 해결이 필요하다. 허용권한이 기술된 권한규칙이 존재하지 않는다면 사용자의 요청은 거부권한이 기술된 규칙이 적용되어 거부권한이 부여된다. 거부권한이 기술된 권한부여 규칙이 존재하지 않는다면 다음으로 허용권한이 기술된 권한부여 규칙이 존재하는지 찾아보고, 있다면 허용권한 규칙이 적용되어 사용자의 요청은 허용권한이 부여된다. 만약, 허용권한과 거부권한이 기술된 규칙이 존재하지 않는다면 사용자의 요청에 대하여 적용될 권한부여 규칙이 존재하지 않으므로 디폴트 규칙(허용 또는 거부)에 따른다.

### 4.4 권한 충돌과 해결방안

권한 충돌이 발생하는 원인은 상황에 따라 역할-서비스-객체 계층에 대한 접근 권한이 기술되기 때문이다. 상황의 계층 구조상에서 하위에서 상위에 존재하는 상황을 고려하여 접근 권한을 평가하기 때문에 같은 역할-서비스-객체에 대하여 서로 다른 권한을 갖는 경우 권한 충돌이 발생한다.

#### 4.4.1 단일 상황에서 발생하는 권한 충돌과 해결방안

단일 상황에서 권한 충돌이 발생하는 원인은 상황 계층 구조상 하위 상황에서 역할-서비스-객체에 대한 권한과 상위 상황에서 역할-서비스-객체에 대한 접근권한이 서로 다른 경우 발생한다.

기존의 방법들에서는 권한 사이에 충돌이 발생하였을 경우 우선 규칙(precedence rule)을 적용하여 처리한다. 우선 규칙이 허용권한이 높은 우선순위를 갖는 경우 허용권한을 적용되고, 거부권한이 높은 우선순위를 갖는 경우 거부권한을 적용한다. 대부분 디폴트 값을 따라 거부권한이 적용된다.

그러나 사용자의 상황을 고려하여 접근제어를 수행하므로 사용자의 상황에 밀접한 접근 권한을 부여하는 것이 적합하다. 단일 상황에서 발생하는 충돌은 사용자의 상황에 가장 가까운 상황의 역할-서비스-객체가 갖는 권

한을 따르도록 함으로써 해결 가능하다.

#### 4.4.2 복합 상황에서 발생하는 권한 충돌과 해결방안

두 개 이상의 상황이 and-결합으로 결합된 복합 상황들의 구성 상황 중에서 부모-자식 관계를 갖는 같은 유형의 상황들이 역할-서비스-객체에 대하여 각각 서로 다른 접근권한을 갖는 경우에 발생한다.

단일 상황에서 발생하는 충돌과 마찬가지로 기존 연구에서는 권한 충돌에 대하여 우선 규칙을 적용하여 처리한다. 상황을 고려하여 접근제어를 수행하므로 상황에 따라 권한을 결정해 줄 수 있다. 각 유형에 대하여 활성화 되어 있는 상황 중에서 사용자의 상황과 가장 가까운 상황에서 역할-서비스-객체가 갖는 권한을 따르도록 함으로써 권한을 결정할 수 있다. 각 유형의 가장 가까운 상황들에 대하여 서로 다른 권한을 부여하는 규칙이 존재하는 경우 권한충돌은 해결되지 않는다. 이러한 경우 우선 규칙을 적용하여 처리한다.

### 4.5 의미 충돌과 해결방안

의미 충돌은 복합 상황 중 AND 상황에서 발생한다. AND 상황을 구성하는 상황들이 서로 상충적인 의미를 가지고 있어 함께 기술되었을 때 발생한다. 예를 들면, 사용자의 위치와 관련한 상황은 하나만 포함될 수 있다. 사용자의 위치 값은 꼭 하나의 값만 참이 될 수 있다. 따라서 둘 이상의 상황이 AND 상황 정의에 이용될 경우 그 상황은 항상 거짓 값을 갖게 된다.

따라서 상충적인 의미를 갖는 상황은 AND 상황에 함께 기술되지 않도록 하는 제약이 필요하다. 상황 계층구조 상에서 같은 레벨에 존재하는 상황을 함께 기술될 수 있는 양립 가능한 상황(compatible context)과 함께 기술될 수 없는 상황(incompatible context)으로 구분할 수 있다.

## 5. 결 론

하드웨어 기술의 발전과 더불어 센서 네트워크는 최근 다양한 환경의 모니터링과 감시를 위한 응용, 침입탐지 및 홈 어플리케이션에 확고한 플랫폼으로 자리 잡고 있다. 정보를 효율적으로 추출하는 동안 복잡한 하위 레벨의 기능에서 벗어나는 응용에 대한 이벤트 서비스를 제공하는 것은 센서 네트워크 상의 응용에서 핵심 기능이다. 추가로 센싱된 데이터를 기반으로 응용의 안전하게 통제하는 상황-인식 기반의 안전한 보안을 제공하는 것 역시 센서 네트워크 상의 응용의 확대를 위해 필수 기능이다.

센서 네트워크는 정보를 수집하고자 하는 어떤 환경 혹은 그 환경 가까이에 대규모로 근접하게 배치되어 정



보를 수집한다. 특히, 사용자가 의식하지 않을 수 있을 만큼의 소형인 센서가 저 전력을 소비하면서 장시간 동작하기 위해서는 모든 환경을 센싱하고 그것을 전송하는 것은 바람직하지 않다.

본 고에서 설명한 LAS는 무선 센서 네트워크 상의 다섯 가지 중요한 특성들을 바탕으로 이벤트를 분류하고 사용자가 자유자재로 관심있는 이벤트를 등록하여 그에 해당되는 센싱 데이터만을 수집하는데 초점을 두고 있다. 비파괴적인 영역 이벤트를 기준으로 시간적으로는 센서 노드의 불규칙적인 패턴의 신뢰성을 위해 시간 윈도우 기반 하에 신뢰 계산을 지원하고 있으며, 공간적으로는 원자적 이벤트 위치 측정을 위한 원자적 영역 합집합 알고리즘과 혼합 이벤트 위치 측정을 위한 원자적 이벤트들 간의 교집합 알고리즘의 개념을 소개하고 있다.

상황-인식과 센서 네트워크와의 접목을 이용하면 센서의 출력 정보를 가지고 이를 수집, 해석하여 그에 따른 적절한 정보와 서비스를 선택적으로 제공하거나 자동으로 실행하는 컴퓨팅 환경을 제공하게 된다. 여기서 중요한 이슈는 생성된 정보와 서비스는 반드시 인가된 사용자들이 공유해야 하며, 그렇지 않은 사용자에게 정보나 서비스가 노출 혹은 변경되지 말아야 한다는 사실이다.

추가로 본 고에서 설명한 CBDAC 모델은 센싱된 상황 정보를 기반으로 정보나 서비스를 관리하는데 초점을 두고 있다. CBDAC 모델은 사용자의 역할과 그 역할에 할당되는 서비스 그리고 그 서비스를 지원하는 자원의 관계에 보안 등급을 부여하고 역할-서비스-객체 관계 사이에 계층 구조를 구성하여 다양하게 변하는 상황 정보에 유연하게 대처할 수 있는 상황 기반의 동적 접근 제어 모델을 제시하고 있다. 그러나 아직은 개발 초기 단계라 권한 부여 규칙을 찾는 탐색 시간의 단축과 빠른 응답 시간을 보장하고 있지 못하다. 한편, 센싱된 상황 정보의 부정확성을 감안한 무조건적인 접근 불허 정책이 아닌 정확도의 등급에 따라 부분 역할을 할당하여 어느 정도의 기본 서비스를 받을 수 있는 부분 서비스, 부분 서비스를 위한 부분 객체의 개념에 대한 추가 연구가 필요하다.

## 참고문헌

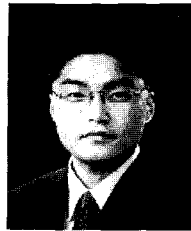
- [1] N. Shrivastava, C. Buragohain, and D. Agrawal, "Medians and Beyond: New Aggregation Techniques for Sensor Networks," In Proc. Of the Second ACM Conf. On Embedded Networked Systems (SenSys), Nov. 2004.
- [2] X. Liu, Q. Huang, and Y. Zhang, "Combs, Needles, Haystacks: Balancing Push and Pull for Discovery in Large-Scale Sensor Networks," In Proc. Of the Second ACM Conf. On Embedded Networked Systems (SenSys), Nov. 2004.
- [3] S. Nath, P. B. Gibbons, Z. R. Anederson, and S. Seshan, "Synopsis Diffusion for Robust Aggregation in Sensor Networks," In Proc. Of the Second ACM Conf. On Embedded Networked Systems (SenSys), Nov. 2004.
- [4] S. Li, Y. Lin, S. H. Son, J. Stankovic, and Y. Wei, "Event Detection Services using Data Service Middleware in Distributed Sensor Networks," Telecommunication Systems, Special Issue on Information Processing in Sensor Networks, vol. 26, no. 2-4, pp 351-368, Aug. 2004.
- [5] S. Madden and M. J. Franklin: "Fjording the stream," "An architecture for queries over streaming sensor data," In ICDE 2002.
- [6] S. Madden and J. M. Hellerstein, "Distributing queries over low-power wireless sensor networks," In SIGMOD 2002.
- [7] Y. Yao and J. Gehrke, "The Cougar Approach to In-Network Query Processing in Sensor Networks," SIGMOD, 2002
- [8] N. Sadagopan, B. Krishnamachari, and A. Helmy, "Active Query Forwarding in Sensor Networks (ACQUIRE)," SNPA' 03, May 2003.
- [9] A. Wood, J. Stankovic, and S. H. Son: JAM, "Jammed Area Mapping Service in Wireless Sensor Networks," 24th IEEE Real-Time Systems Symposium (RTSS'03), Cancun, Mexico, Dec. 2003.
- [10] R. Nowak and U. Mitra, "Boundary estimation in sensor networks: Theory and methods," IPSN'03, Apr. 2003.
- [11] J. M. Hellerstein, W. Hong, S. Madden, and K. Stanek, "Beyond average: Towards sophisticated sensing with queries," IPSN '03, Mar. 2003.
- [12] Amol Bakshi, Mitali Singh and Viktor K. Prasanna, "Supporting Topographic Queries in Sensor Networks," Tech Rep CENG-

2003-04, Dept of EE-Systems, Univ. of Southern California, Dec. 2003

- [13] D. Devaguptapu and B. Krishnamachari, "Applications of localized image processing techniques in wireless sensor networks," In Aerosense, April 2003.
- [14] M. J. Covington, M.J. Moyer and M. Ahamad, "Generalized Role-based Access Control for Securing Future Applications," In 23rd National Information Systems Security Conference (NISSC), pp.115-125, Baltimore, Maryland, USA, October 2000.
- [15] Michael J. Covington, Prahlad Fogla, Zhiyuan and Mustaque Ahamad, "A Context-Aware Security Architecture for Emerging Applications," In 18th Annual Computer Security Applications Conference (ACSAC2002), Las Vegas, Nevada, USA, December 2002.
- [16] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman, "Role Based Access Control Model," In IEEE Computer 20(2), pp.38-47, February 1996.
- [17] Gustaf Neumann and Mark Strembeck, "An Approach to Engineer and Enforce Context Constraints in an RBAC Environment," In 8th ACM Symposium on Access Control Models and Technologies (SACMAT2003), pp. 65-79, Como, Italy, June 2003.
- [18] Matthew J. Moyer and Mustaque Ahamad, "Generalized Role-based Access Control," In IEEE International Conference on Distributed Computing Systems(ICDCS 2001), pp.391-398, Mesa, Arizona, USA, April 2001.
- [19] M. Wilikens, S. Feriti, A. Sanna and M. Masera, "A Context-Related Authorization and Access Control Method Based on RBAC : A case study from the health care domain," In 7th ACM Symposium on Access Control Models and Technologies (SACMAT2002), pp.117-124, 2002.

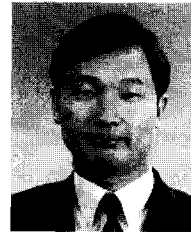
---

### 변 창 우



1999 서강대학교 컴퓨터학과(학사)  
2001 서강대학교 컴퓨터학과(석사)  
2001~현재 서강대학교 컴퓨터학과 박사 과정  
관심분야: Transaction Management for Dynamic Database, Role-based Access Control, Context-awareness Access Control  
E-mail : chang@dblab.sogang.ac.kr

### 박 석



1978 서울대학교 계산통계학과(이학사)  
1980 한국과학기술원 전산학과(공학석사)  
1983. 8 한국과학기술원 전산학과(공학박사)  
1983. 9~현재 서강대학교 컴퓨터학과 교수  
1999~현재 DASFAA Steering Committee  
2002~2003 University of Virginia 방문교수  
1998~현재 한국정보과학회 데이터베이스연구회 운영자문위원  
2004. 1~현재 한국정보과학회 상임이사  
2004. 1~현재 한국정보과학회지 편집위원장  
2004. DASFAA 2004 Organization Chair  
관심분야: Database Security, Transaction Management, XML, Streaming Data Processing, Ubiquitous Computing, Role-based Access Control, Context-awareness Access Control  
E-mail: spark@sogang.ac.kr

### 손 상 혁



1976 서울대학교 전자공학과(학사)  
1982 한국과학기술원 전산학과(공학석사)  
1986 University of Maryland(박사)  
1986~현재 Professor of Computer Science at University of Virginia  
1998~2001 Associate Editor of the IEEE Transactions on Parallel and Distributed Systems  
Guest editor for the ACM SIGMOD Record, Special Issue on Real-Time Database Systems,  
Guest editor for the IEEE Trans. on Software Engineering, Special Section on Real-Time Systems,  
현재 Editorial board of the Real-Time Systems Journal  
현재 Editor of Journal of Business Performance Management  
관심분야: Real-time computing, database systems, QoS management, data services in embedded and mobile networks, and information security.  
E-mail : son@cs.virginia.edu

---